A TWO-FOLD GENERALIZATION OF FERMAT'S THEOREM.

Presented to the American Mathematical Society, February 29, 1896.

BY PROFESSOR ELIAKIM HASTINGS MOORE.

Formulation of the generalized Fermat theorem $\mathrm{III}[k+1, n; p]$. §§ 1–4.

1. In *Gauss's* congruencé notation *Fermat's theorem* is:

I_1 $$a^p - a \equiv 0 \pmod{p}$$

where p *is any prime and* a *is any integer:*
or, otherwise expressed,

I_2 *The two rational integral functions of the indeterminate* X *with integral coefficients*

$$X^p - X, \quad \prod_{a=0}^{a=p-1} (X+a)$$

are identically congruent ($\equiv$) (mod p):

$$X^p - X \equiv \prod_{a=0}^{a=p-1} (X+a) \pmod{p}.$$

We write I_2 thus:

I_3 *The two forms in the two indeterminates* X_0, X_1,

$$D[2,1;p](X_0, X_1) \equiv X_0 X_1^p - X_0^p X_1,$$

$$P[2,1;p](X_0, X_1) \equiv X_0 \cdot \prod_{a_0=0}^{a_0=p-1} (a_0 X_0 + X_1),$$

are identically congruent (mod p):

$$D[2,1;p](X_0, X_1) \equiv P[2,1;p](X_0, X_1) \pmod{p}.$$

2. We proceed in two steps to a two-fold generalization of Fermat's theorem I_3.

II. *The two forms in the* $k+1$ *indeterminates* $X_0, X_1, \cdots, X_k$,

(1) $D[k+1, 1; p](X_0, X_1, \cdots, X_k) \equiv |X_j^i|$ $\quad (i, j = 0, 1, \cdots, k)$,

(2) $P[k+1, 1; p](X_0, X_1, \cdots, X_k) \equiv \Pi^* \sum_g a_g X_g$ $\quad (g = 0, 1, \cdots, k)$,

—where the product Π^* *embraces the* $(p^{k+1}-1)/(p-1)$ *linear forms* $\sum_{g=0}^{g=k} a_g X_g$ *whose coefficients* a_g $(g=0, 1, \cdots, k)$ *are integers selected from the series* $0, 1, \cdots, p-1$, *in all possible ways, only*

so that for every particular form, first, the coefficients a_g are not all 0, *and, second, of the coefficients a_g not* 0 *the one with largest index* g *is* 1 —— *are identically congruent* (mod p):

$$D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv P[k+1, n; p](X_0, X_1, \cdots, X_k).$$

When we collect into a *class* the totality of integers congruent to one another (mod p), and denote the p incongruent classes by p *marks*, we have in this system of p marks a *field* $F[p]$ *of order* p *and rank* 1. The marks of the field $F[p]$ may be combined by the four fundamental operations of algebra—addition, subtraction, multiplication, division, —the operations being subject to the ordinary abstract operational laws of algebra, the results of these operations being in every case uniquely determined and belonging to the field. *Congruences* ($\equiv$) (mod p) are in the field *equalities* ($=$), and *identical congruencies* ($\equiv\!\!\!\equiv$) are *identities* ($\equiv$). The restatement of II in the terminology of the field $F[p]$ is given by setting $n=1$ in its generalization III (§ 3).

3. The second step of generalization of I_3 rests upon *Galois's* generalization of the field $F[p]$ to the *Galois-field* $GF[p^n]$ of *order* p^n, *modulus* p, *and rank* n. This field of p^n marks α is uniquely defined for every p=prime, n=positive integer. (I have elsewhere proved that every field of finite order s is a Galois-field of order $s=p^n$.)

A form, that is, a rational integral function of certain indeterminates, $X_0, X_1, \cdots, X_k$, is said to *belong* to the $GF[p^n]$ if its coefficients belong to (are marks α of) the $GF[p^n]$. A *linear homogeneous form* $\sum_{g=0}^{g=k} a_g X_g$ belonging to the $GF[p^n]$ is called *primitive* if not all its coefficients a_g are 0, and if of the coefficients a_g not 0 the one with largest index g is 1.

We have then:

III. *The two forms in the* $k+1$ *indeterminates,* $X_0, X_1, \cdots, X_k$,

$$(3)\quad D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv X_j^{p^{ni}} \qquad (i, j = 0, 1, \cdots, k),$$

$$(4)\quad P[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv \prod{}^{*} \sum_g a_g X_g \qquad (g = 0, 1, \cdots, k),$$

—where the product $\prod^*$ *embraces the* $(p^{n(k+1)}-1)/(p^n-1)$ *distinct primitive linear homogeneous forms* $\sum_{g=0}^{g=k} a_g X_g$ *belonging to the* $GF[p^n]$ *— are identical:*

$$D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv P[k+1, n; p](X, X_1, \cdots, X_k).$$

The forms D, P whose identity theorem III affirms have the three characteristic positive integers or *characters* $k+1$, n, p. It is convenient to attach these characters to the no-

tation III for the theorem, and thus to speak of the theorem $\mathrm{III}[k+1, n; p]$. This theorem requires proof only for $k \geq 1$, since for $k = 0$, $D \equiv X_0$, $P \equiv X_0$.

4. For the proof of $\mathrm{III}[k+1, n; p]$ we need *Galois's* one-fold generalizations of the *Fermat theorems* I:

II_1' *Every mark* α *of the* $GF[p^n]$ *satisfies the equation*

$$\alpha^{p^n} - \alpha = 0.$$

whence,

II_2' *The two forms in the indeterminate* X

$$X^{p^n} - X, \qquad \prod_{\alpha \mid p^n} (X + \alpha)$$

belonging to the $GF[p^n]$ *are identical:*

$$X^{p^n} - X \equiv \prod_{\alpha \mid p^n} (X + \alpha),$$

(where, as always, the subscript-remark $\alpha \mid p^n$ means that the mark α is to run over the p^n marks of the $GF[p^n]$), and further,

II_3' *The two forms in the two indeterminates* X_0 X_1,

$$D[2, n; p](X_0, X_1) \equiv X_0 X_1^{p^n} - X_0^{p^n} X_1,$$
$$P[2, n; p](X_0, X_1) \equiv \prod{}^{*} (a_0 X_0 + a_1 X_1),$$

— *where the product* $\prod^*$ *embraces the* p^n+1 *distinct primitive linear homogeneous forms* $a_0 X_0 + a_1 X_1$ *belonging to the* $GF[p^n]$ — *are identical:*

$$D[2, n; p](X_0, X_1) \equiv P[2, n; p](X_0, X_1).$$

A (known) corollary to II_1' is also needed. We denote by Λ_k the substitution on the p^n marks α of the $GF[p^n]$ which replaces every mark α by α^{p^k}; obviously $\Lambda_c \Lambda_d = \Lambda_{c+d}$ while by II_1', $\Lambda_n = \Lambda_0 = 1$. We denote by $F_k(X_0, X_1, \cdots, X_k)$ the result obtained by applying the substitution Λ_k to the mark-coefficients of a form $F(X_0, X_1, \cdots, X_k)$ belonging to the $GF[p]$, so that $F_n(X_0, X_1, \cdots, X_k) \equiv F_0(X_0, X_1, \cdots, X_k) \equiv F(X_0, X_1, \cdots, X_k)$. Since in the involution of a multinomial to the p^{th} power the say *intermediate* multinomial coefficients are all divisible by p, we have in the $GF[p^n]$ of modulus p,

$$F_k(X_0, X_1, \cdots, X_k)^p \equiv F_{k+1}(X_0^p, X_1^p, \cdots, X_k^p),$$

whence

II_1' Cor. $\quad F(X_0, X_1, \cdots, X_k)^{p^n} \equiv F(X_0^{p^n}, X_1^{p^n}, \cdots, X_k^{p^n})$,

where $F(X_0, X_1, \cdots, X_k)$ *is any form of the* $GF[p^n]$.

The theorem III$[k+1, n; p]$ bears the same relation to Galois's Fermat's theorem II$'$: $\mathrm{II}_3' \equiv \mathrm{III}[2, n; p]$: that the theorem II $\equiv$ III$[k+1, 1; p]$ bears to Fermat's theorem I : $\mathrm{I}_3 \equiv \mathrm{III}[2, 1; p]$. I am communicating then one-fold generalizations II, III of the known theorems I, II$'$; of these II may be looked at as a theorem in the ordinary Gauss-congruence theory, while its generalization III is a theorem in the Galois-field theory.

I give three proofs A, B, C of the general theorem III$[k+1, n; p]$. The proof A depends upon considerations involving the $GF[p^n]$ of rank n alone, and accordingly for $n=1$ this proof A of III$[k+1, 1; p] \equiv$ II may be exhibited in the terminology of the ordinary Gauss-congruence theory. The proofs B and C however depend upon considerations involving the wider $GF[p^{mn}]$ of rank mn $(m \geq 2k^2)$; they throw a sharper light upon the essential meaning of the theorem III$[k+1, n; p]$ for every n.

Proof A of the theorem III $[k+1, n; p]$. § 5.

Proof by two-based induction. We know that III$[1, n; p]$ and III$[2, n; p] \equiv \mathrm{II}_3'$ are true. On the supposition that III$[l-1, n; p]$ and III$[l, n; p]$ $(l > 1)$ are true we prove that III$[l+1, n; p]$ is true.

5. In the determinant $U = |\, u_{ij} \,|\, (i, j = 0, 1 \cdots\cdots, l)$ we denote by U_{ij} the minor complementary to u_{ij}, and have*

$$(5) \qquad (-1)^{l+1} \begin{vmatrix} U_{11}, & U_{10} \\ U_{01}, & U_{00} \end{vmatrix} \equiv U. \,|\, u_{ij} \,| \quad \left(\begin{smallmatrix} i=1, 2 \cdots, l-1 \\ j=2, 3, \cdots, l \end{smallmatrix}\right)$$

We set now

$$u_{ij} = X_j^{p^i} \qquad (i, j = 0, 1, \cdots, l),$$

so that we have

$$(6) \quad \begin{aligned} &D[l+1, n; p](X_0, X_1, \cdots, X_l) \equiv + U, \\ &D[l-1, n; p](X_2^{p^n}, X_3^{p^n}, \cdots X_l^{p^n}) \equiv |\, u_{ij} \,| \ \left(\begin{smallmatrix} i=1, 2, \cdots, l-1 \\ j=2, 3, \cdots, l \end{smallmatrix}\right), \\ &D[l, n; p](X_0, X_2, \cdots, X_l) \equiv (-1)^{l+1} U_{11}, \\ &D[l, n; p](X_1, X_2, \cdots, X_l) \equiv (-1)^{l} U_{10}, \\ &D[l, n; p](X_0^{p^n}, X_2^{p^n}, \cdots, X_l^{p^n}) \equiv - U_{01}, \\ &D[l, n; p](X_1^{p^n}, X_2^{p^n}, \cdots, X_l^{p^n}) \equiv + U_{00}. \end{aligned}$$

Then by substituting the values (6) in the identity (5) and remembering II$_1'$ Cor. and the definition (3) of $D[2, n; p]$ (Y_0, Y_1), we have the fundamental identity

* See, for instance, Scott's *Determinants*, p. 57, No. 6.

$$(7)\quad D[2,n;p]\Big(D[l,n;p](X_0,X_2,\cdots,X_l),D[l,n;p](X_1,X_2,\cdots X_l)\Big)$$
$$\equiv D[l+1,n;p](X_0,X_1,\cdots,X_l)\cdot D[l-1,n;p](X_2,X_3,\cdots X_l)^{p^n}.$$

Now, using always the Π^* in the sense defined in the enunciation of III, we have by hypothesis :

$$(8_1)\ \mathrm{III}[2,n;p]:\ D[2,n;p](Y_0,Y_1)\equiv P[2,n;p](Y_0,Y_1)\equiv \Pi^*(\beta_0 Y_0+\beta_1 Y_1)\equiv Y_0\cdot\prod_{\beta\,|\,p^n}(\beta Y_0+Y_1),$$

$$(8_2)\ \mathrm{III}[l-1,n;p]:\ D[l-1,n;p](Y_0,Y_1,\cdots,Y_{l-2})\equiv P[l-1,n;p](Y_0,Y_1,\cdots,Y_{l-2})\equiv\Pi^*\sum_{h=0}^{h=l-2}\beta_h Y_h,$$

$$(8_3)\ \mathrm{III}[l,n;p]:\ D[l,n;p](Y_0,Y_1,\cdots,Y_{l-1})\equiv P[l,n;p](Y_0,Y_1,\cdots,Y_{l-1})\equiv\Pi^*\sum_{h=0}^{h=l-1}\beta_h Y_h.$$

By (8_2) the left side of the identity (7) is

$$(9)\quad D[l,n;p](X_0,X_2,\cdots,X_l)\cdot\prod_{\beta\,|\,p^n}\Big(\beta\,D[l,n;p](X_0,X_2,\cdots,X_l)+D[l,n;p](X_1,X_2,\cdots,X_l)\Big),$$

which, using II_1' and II_1' Cor. in the addition of the determinants, is

$$(10)\quad D[l,n;p](X_0,X_2,\cdots,X_l)\cdot\prod_{\beta\,|\,p^n}D[l,n;p](\beta X_0+X_1,X_2,\cdots,X_l),$$

which by (8_3) is

$$(11)\quad \Pi^*(\delta_0 X_0+\delta_2 X_2+\cdots+\delta_l X_l)\cdot\prod_{\beta\ p^n}\Pi^*\Big(\gamma_1(\beta X_0+X_1)+\gamma_2 X_2+\cdots+\gamma_l X_l\Big).$$

We compare the product (11) with the product (12),

$$(12)\quad P[l+1,n;p](X_0,X_1,\cdots,X_l)\equiv\Pi^*(\alpha_0 X_0+\alpha_1 X_1+\alpha_2 X_2+\cdots+\alpha_l X_l).$$

The factors of (12) are the primitive linear homogeneous forms $\sum_{g=0}^{g=l}\alpha_g X_g$ with no omissions and no repetitions. Every factor of (11) is likewise such a form. And in (11) every such form $\sum_{g=0}^{g=l}\alpha_g X_g$ occurs at least once; any such form $\sum_{g=0}^{g=l}\alpha_g X_g$

with $a_1 \neq 0$ occurs (since $l > 1$) once and only once, viz., under that $\prod^*$ of the second set in (11) whose forms have $\beta = a_0 / a_1$; any such form $\sum_{g=0}^{g=l} a_g X_g$ with $a_1 = 0$, $a_0 \neq 0$, occurs once and only once, viz., under the single $\prod^*$ of the first set in (11); any such form $\sum_{g=0}^{g=l} a_g X_g$ with $a_1 = 0$, $a_0 = 0$, occurs in all $1 + p^n$ times, viz., once and of course only once under every $\prod^*$ of (11). Thus the product (11) is:

$$(13) \quad P[l+1, n; p](X_0, X_1, \cdots, X_l) \cdot \left(\prod{}^* \sum_{g=1}^{g=l} a_g X_g \right)^{p^n}.$$

When we substitute (13) for the left side of the identity (7) and divide out* the second factors, which are identical by the hypothesis (8_2), we have the desired identity

$$(14) \quad \mathrm{III}[l+1, n; p]: \quad P[l+1, n; p](X_0, X_1, \cdots, X_l) \equiv D[l+1, n; p](X_0, X_1, \cdots, X_l).$$

Proof B of the theorem $\mathrm{III}[k+1, n; p]$. §§ 6–11.

Direct proof of the identity $\mathrm{III} \leftrightarrows [k+1, n; p]$

$$\mathrm{III} \leftrightarrows \quad D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv$$

$$D[k, n; p](X_0, X_1, \cdots, X_{k-1}) \cdot \prod_{\substack{a_r \mid p^n \\ (r=0, \cdots, k-1)}} \left(\sum_{r=0}^{r=k-1} a_r X_r + X_k \right).$$

6. *From the identity* $\mathrm{III} \leftrightarrows [l+1, n; p]$ *for* $l = 1, 2, \cdots, k$, *and in view of the definition* (3) $D[1, n; p](X_0) \equiv X_0$, *we have*

$$(15) \quad D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv X_0 \cdot \prod_{l=1}^{l=k} \prod_{\substack{a^r \mid p^n \\ (r=0, \cdots, l-1)}} \left(\sum_{r=0}^{r=l-1} a_r X_r + X_l \right),$$

viz., *the identity called for by the theorem* $\mathrm{III}[k+1, n; p]$.

7. *We introduce the* $GF[p^{mn}]$ *of modulus* p *and rank* mn *where* m *is any integer* $m \geq 2k^2 \geq k+1$. The $GF[p^{mn}]$ contains the $GF[p^n]$. The forms entering the theorems $\mathrm{III}[k+1, n; p]$, $\mathrm{III} \leftrightarrows [k+1, n; p]$ belong to the $GF[p^n]$, and the theorems then to the $GF[p^n]$-theory, but the forms belong also to the wider $GF[p^{mn}]$, and the proofs B, C of $\mathrm{III} \leftrightarrows$ and III make use of this fact.

*As to the fact that the quotient-forms so obtained are identical, see, for instance, the theorem (3) § 3 of the memoir by WEBER: *Die allgemeinen Grundlagen der Galoisschen Gleichungstheorie* (*Mathematische Annalen*, vol. 43, pp. 521–549, 1893.)

8. The small Greek letters $\alpha, \beta, \gamma, \cdots$, as heretofore designate marks of the $GF[p^n]$, and the large Greek letters A, B, Γ, $\cdots$. marks of the $GF[p^{mn}]$.

Any t marks A_r $(r=1, 2, \cdots, t)$ of the $GF[p^{mn}]$ determine in the $GF[p^{mn}]$ an *additive-group* $[A_1, A_2, \cdots, A_t \mid GF[p^n]]$ with the *basis-system* $A_1, A_2, \cdots, A_t$ and *field of reference* $GF[p^n]$ containing all possible marks A expressible in the form

$$A = \sum_{r=1}^{r=t} \alpha_r A_r \tag{16}$$

where the $\alpha_r (r=1, 2, \ldots, t)$ are marks of the field of reference $GF[p^n]$.

The p^{tn} marks A(16) are distinct if the particular mark $A = 0$ occurs only once, viz., with the coefficients α_r all 0. In this case, when of course $t \leq m$, the additive-group has the *order* p^{tn} and *rank* t, and the t marks A_r are *linearly independent with respect to* * *the* $GF[p^n]$, and obviously any t' of the t marks are likewise linearly independent. If $t<m$, not all the marks of the $GF[p^{mn}]$ are in this additive-group of rank t, and any external mark A_{t+1} forms with the t marks A_r a system of $t+1$ linearly independent marks, and thus extends the additive-group of rank t to one of rank $t+1$. We take as a start any mark $A_1 \neq 0$, and by the preceding remarks may affirm: (a) There exist systems of l marks $A_1, A_2, \cdots, A_l$ of the $GF[p^{mn}]$ linearly independent with respect to the $GF[p^n]$ for every $l, l = 1, 2, \cdots, m$; (b) every additive-group $[A_1, A_2 \cdots, A_t \mid GF[p^n]]$ may be exhibited as an additive-group of some rank $l \leq t$ based upon such a system of l linearly independent marks chosen from amongst the original t basal marks A_r.

9. We take now any system of $k+1$ (not necessarily distinct) marks B_g $(g=0, 1, \cdots, k)$ of the $GF[p^{mn}]$ and consider the two marks

$$\Delta \equiv D[k+1, n; p]\,(B_0, B_1, \ldots B_k) \equiv |B_j^{p^{ni}}| \quad (i, j=0, \cdots, 1, k), \tag{17}$$

$$\Pi \equiv P[k+1, n; p](B_0, B_1, \cdots, B_k) \equiv \Pi^* \sum_g \alpha_g B_g \quad (g=0, 1, \cdots, k). \tag{18}$$

Clearly $\Pi = 0$ if and only if the marks B_g are linearly dependent. And further, since from an equation,

$$\sum_{j=0}^{j=k} \alpha_j B_j = 0,$$

*In the sequel the $GF[p^n]$ is always the field of reference.

we have, by II_1' Cor., the $k+1$ equations,

$$\left(\sum_{j=0}^{j=k} a_j B_j\right)^{p^{mi}} \equiv \sum_{j=0}^{j=k} a_j B_j^{p^{mi}} = 0 \qquad (i=0, 1, \cdots, k).$$

we see that if the marks B_g are linearly dependent, then $\Delta = 0$.

(In passing we notice that the remark just made concerning Π and the theorem $\mathrm{III}[k+1, n; p]$ yield the theorem:

A necessary and sufficient condition that $k+1$ marks B_g $(g=0, 1, \cdots, k)$ of a $GF[p^{mn}]$ (m any integer) shall be linearly dependent with respect to the $GF[p^n]$ is the vanishing of the determinant $\Delta \equiv |B_j^{p^{mi}}|$ $(i, j=0, 1\cdots, k)$. (If $m < k+1$, then Δ vanishes for every system of $k+1$ marks B_g). This yields its still more important corollary:

The rank of the additive-group $[B_0, B_1\cdots, B_k \mid GF[p^n]]$ *is the same as the rank of the matrix* $(B_j^{p^{mi}})$ $(i, j=0, 1, \cdots, k)$, where a matrix (u_{ij}) $(^{i=0, 1, \ldots, k}_{j=0, 1, \ldots, l})$ is said to have the *rank* r if its every sub-determinant of order $r' > r$ vanishes while at least one sub-determinant of order $r' = r$ does not vanish.

It would not be difficult to establish this theorem and its corollary independently of the theorem $\mathrm{III}[k+1, n; p]$.)

10. Next we consider a system of $k(k+1 \leqq m)$ linearly independent marks A_r $(r=0, 1, \cdots, k-1)$, and select from the p^{kn} marks A of the additive-group $[A_1, A_2\cdots, A_k \mid GF[p^n]]$ any $k+1$ marks B_g $(g=0, 1, \cdots, k)$. These marks B_g are linearly dependent, for otherwise the additive-group based on them would have the order $p^{(k+1)n}$, whereas it is contained in the additive-group of order p^{kn} based on the k marks A_r. For these marks B_g then (§ 9) $\Delta = 0$, $\Pi = 0$, and so

$$(19)\quad D[k+1, n; p](B_0, B_1, \cdots, B_k) = P[k+1, n; p](B_0, B_1, \cdots, B_k).$$

11. We take now any system of $2k^2 (2k^2 \leqq m)$ linearly independent marks E_{rs} $(^{r=0, 1, \ldots, k-1}_{s=1, 2, \ldots, 2k})$ and split it up at once into k systems of $2k$ linearly independent (§8) marks.

The system E_{rs} $(s=1, 2, \cdots 2k)$ determines the additive-group $[E_{r1}, E_{r2}, \cdots, E_{r2k} \mid GF[p^n]]$ containing besides the mark 0 $p^{2kn}-1$ marks A_r of the form $A_r = \sum_{s=1}^{s=2k} \varepsilon_{rs} E_{rs}$, where the ε_{rs} are marks of the $GF[p^n]$ not all 0. We select from each additive-group any mark A_r $(A_r \neq 0)$ $(r=0, 1, \cdots, k-1)$. These k marks A_r are linearly independent, and determine the additive-group $[A_0, A_1, \cdots, A_{k-1} \mid GF[p^n]]$ containing

p^{kn} marks A of the form $A=\sum_{r=0}^{r=k-1} a_r A_r$. By §10 we have for every such mark A

$$D[k+1, n; p](A_0, A_1, \cdots, A_{k-1}, A)=0. \tag{20}$$

Hence the equation for X_k

$$D[k+1, n; p](A_0, A_1, \cdots, A_{k-1}, X_k)=0. \tag{21}$$

which is of degree p^{kn} in the unknown X_k with the leading coefficient $D[k, n; p](A_0, A_1, \cdots, A_{k-1})$ has as roots the p^{kn} marks A of the form $A=\sum_{r=0}^{r=k-1} a_r A_r$. Since the marks A are given equally well in the form $A=-\sum_{r=0}^{r=k-1} a_r A_r$, we have the identity in the indeterminate X_k:

$$D[k+1, n; p](A_0, A_1, \cdots, A_{k-1}, X_k)\equiv \tag{22}$$

$$D[k, n; p](A_0 A_1 \cdots A_{k-1})\cdot \prod_{\substack{a_r \\ (r=0, 1, \ldots, k-1,} \mid p^n} \left(\sum_{r=0}^{r=k-1} a_r A_r + X_k\right).$$

Now consider the two forms in the $k+1$ indeterminates $X_0, X_1, \cdots, X_k$:

$$D[k+1, n; p](X_0, X_1, \cdots, X_{k-1}, X_k), \tag{23}$$

$$D[k, n; p](X_0, X_1, \cdots, X_{k-1})\cdot \prod_{\substack{a_r \\ (r=0, \ldots, k-1)} \mid p^n} \left(\sum_{r=0}^{r=k-1} a_r X_r + X_k\right).$$

We affirm their identity: this is the theorem III $\fallingdotseq [k+1, n; p]$. Denoting by $C(X_0, X_1, \cdots, X_{k-1})$, $C'(X_0, X_1, \cdots, X_{k-1})$ the coefficients of any certain same power of X_k in the respective forms (23), we prove the identity in the k indeterminates $X_0, X_1, \cdots, X_{k-1}$:

$$C(X_0, X_1, \cdots, X_{k-1}) \equiv C'(X_0, X_1, \cdots, X_{k-1}). \tag{24}$$

In the first place these forms are of degree $\leqq p^{kn}$ in each indeterminate. Further by (22)

$$C(A_0, A_1, \cdots, A_{k-1})=C'(A_0, A_1, \cdots, A_{k-1}) \tag{25}$$

where for $r=0,1,\cdots,k-1$ A_r is any of the $p^{2kn}-1 (p^{2kn}-1>p^{kn})$ marks $A_r \neq 0$ of the additive-group $[E_{r1}, E_{r2}, \cdots, E_{r2k} \mid GF[p^n]]$. The desired identity (24) follows then by the *identity-theorem* (which is proved in the Galois-field theory just as is the corresponding theorem in the theory of the ordinary general algebraic field):

Identity-theorem. If the two forms of the $GF[p^{mn}]$

$$C(Y_1, Y_2, \cdots, Y_l), \quad C'(Y_1, Y_2, \cdots, Y_l)$$

contain the l indeterminates $Y_1, Y_2, \cdots, Y_l$ to degrees respectively less than the numbers $y_1, y_2, \cdots, y_l$, and if to each indeterminate Y_h $(h=1, 2, \cdots, l)$ a certain system of y_h distinct marks A_h may be associated in such a way that the two marks obtained from the two forms by substituting for each indeterminate Y_h any mark A_h of its associated set are equal:

$$C(A_1, A_2, \cdots, A_l) = C'(A_1, A_2, \cdots, A_l):$$

then the two forms are identical:

$$C(Y_1, Y_2, \cdots, Y_l) \equiv C'(Y_1, Y_2, \cdots, Y_l).$$

Proof C of the theorem III $[k+1, n; p]$. §§ 12–14.

Proof by one-based induction. We know that III$[2, n; p] \equiv$ II$_n'$ is true. On the supposition that III $[l, n; p]$ $(l>1)$ is true we prove that III$[l+1, n; p]$ is true.

12. By interchanging two adjacent columns of the determinant $| X_j^{p^{ni}} |$ $(i, j=0, 1, \cdots, l)$ we have:

$$D[l+1, n; p](\cdots, X_h, X_{h+1}, \cdots) \equiv -D[l+1, n; p](\cdots, X_{h+1}, X_h, \cdots). \tag{26}$$

13. To prove the corresponding property for the product $P[l+1, n; p](X_0, X_1, \cdots, X_l)$ we need the Galois-field generalization of *Wilson's theorem:*

$$\text{II}_2' \text{ Cor. } 1 \qquad \prod_{a \mid p^n}{}' a = -1 \qquad (a \neq 0),$$

whence

$$\text{II}_2' \text{ Cor. } 2 \qquad \prod_{a \mid p^n}{}' a^{p^{hn}} = -1 \qquad (a \neq 0)\ (h \text{ any integer}),$$

even for $p=2$, since in a Galois field of modulus $p=2$ the marks $+1, -1$ are equal.

In view of the definition (4) the two products

$$P[l+1, n; p](\cdots, X_h, X_{h+1}, \cdots), \quad P[l+1, n; p](\cdots, X_{h+1}, X_h, \cdots) \tag{27}$$

obviously differ only in the factors $\sum_{g=0}^{g=l} \alpha_g X_g$, $\sum_{g=0}^{g=l} \beta_g X_g$ containing both X_h and X_{h+1} and no X_g with $g>h+1$, that is, in the products

$$\prod_{\substack{a \mid p^n \\ (a \neq 0)}}{}' \prod_{\substack{\alpha_g \mid p^n \\ (g=0, \ldots, h-1)}} \left(\sum_{g=0}^{g=h-1} \alpha_g X_g + \alpha X_h + X_{h+1} \right), \tag{28}$$

$$\prod_{\substack{\beta \mid p^n \\ (\beta \neq 0)}}{}' \prod_{\substack{\beta_g \mid p^n \\ (g=0, \ldots, h-1)}} \left(\sum_{g=0}^{g=h-1} \beta_g X_g + \beta X_{h+1} + X_h \right).$$

Setting, for any $\alpha \neq 0$, $\beta = 1/\alpha$, $\beta_g = \alpha_g/\alpha$ $(g = 0, 1, \cdots, h-1)$, we find easily that the first product (28) is the second product (28) multiplied by $\prod'_{\alpha \mid p^{h_n}} \alpha^{p^{h_n}} (\alpha \neq 0)$, *i. e.*, ($\mathrm{II}_2'$ Cor. 2) by -1.

Hence indeed :

$$P[l+1, n; p](\cdots, X_h, X_{h+1}, \cdots) \equiv -P[l+1, n; p](\cdots, X_{h+1}, X_h, \cdots). \tag{29}$$

We have from (26) (29):

$$D[l+1, n; p](X_0, \cdots, X_{h-1}, X_h, X_{h+1}, \cdots, X_l) \equiv (-1)^{l-h} D[l+1, n; p](X_0, \cdots, X_{h-1}, X_{h+1}, \cdots, X_l, X_h), \tag{30}$$

$$P[l+1, n; p](X_0, \cdots, X_{h-1}, X_h, X_{h+1}, \cdots, X_l) \equiv (-1)^{l-h} P[l+1, n; p](X_0, \cdots, X_{h-1}, X_{h+1}, \cdots, X_l, X_h). \tag{31}$$

14. Now the two forms

$$D[l+1, n; p](X_0, X_1, \cdots, X_l), P[l+1, n, p](X_0, X_1, \cdots, X_l) \tag{32}$$

are of degree p^{ln} in each of the $l+1$ indeterminates X_h $(h = 0, 1, \cdots, l)$; the respective coefficients of $X_l^{p^{nl}}$ are obviously

$$D[l, n; p](X_0, X_1, \cdots, X_{l-1}), P[l, n; p](X_0, X_1, \cdots, X_{l-1}), \tag{33}$$

and hence by (30, 31, 33) the respective coefficients of $X_h^{p^{nl}}$ $(h = 0, 1, \cdots, l)$ are

$$(-1)^{l-h} D[l, n; p](X_0, \cdots X_{h-1}, X_{h+1}, \cdots, X_l), \quad (-1)^{l-h} P[l, n; p](X_0, \cdots, X_{h-1}, X_{h+1}, \cdots, X_l). \tag{34}$$

From (34) and our hypothesis that III $[k+1, n; p]$ is true for $k+1 = l$ it follows that the form

$$D[l+1, n; p](X_0, X_1, \cdots, X_l) - P[l+1, n; p](X_0, X_1, \cdots, X_l) \tag{35}$$

is of degree less than p^{ln} in each of the $l+1$ indeterminates X_h $(h = 0, 1, \cdots, l)$. We take in the $GF[p^{mn}]$ $(m \geq k \geq l)$ any system of l marks A_r $(r = 0, 1 \cdots, l-1)$ linearly independent with respect to the $GF[p^n]$, and associate with each indeterminate X_h $(h = 0, 1, \cdots, l)$ the p^{ln} marks $A = B_h$ of the additive-group based on the marks A_r. Then, since by § 10 (19) for every such system of $l+1$ (linearly dependent) marks B_h $(h = 0, 1, \cdots, l)$ we have

$$D[l+1, n; p](B_0, B_1, \cdots, B_l) - P[l+1, n; p](B_0, B_1, \cdots B_l) = 0, \tag{36}$$

by the identity-theorem (§ 11) we have the desired identity III$[l+1, n; p]$:

$$D[l+1, n; p](X_0, X_1, \cdots, X_l) - P[l+1, n; p](X_0, X_1, \cdots, X_l) \equiv 0.$$

THE UNIVERSITY OF CHICAGO,
January 30, 1896.

ON THE RUFFINI-ABELIAN THEOREM.

BY PROFESSOR J. PIERPONT.

Gauss having rigorously established in 1799 the fundamental theorem of algebra that every equation of degree n possesses n roots real or imaginary,* it was natural to inquire more closely into the nature of these quantities. When n was less than five, it had long been known that these roots could in every case be expressed as explicit algebraic functions of the coefficients; further it was known that for every degree equations existed of more or less special nature for which this was still true. The unsuccessful attempts of the foremost mathematicians of the century which was just closing to find such expressions for the equation of degree five, when the coefficients were left indeterminate, had rendered it very doubtful if the roots of the general equation of degree greater than four possessed this property. Between the years 1799 and 1813 an Italian mathematician, Ruffini,† made several attempts to establish the justice of these doubts; but his reasoning although highly interesting and valuable is not conclusive, and the question remained open until the publication of Abel's ‡ celebrated argument in 1826, where he proved that it was impossible to express the roots of an equation of degree greater than four, as explicit algebraic functions of the coefficients when these last were left indeterminate.

Abel's demonstration, however, is not all that could be desired. In the first place, as he was ignorant of Ruffini's beautiful researches, the substitution-theoretical part of his paper is unnecessarily roundabout; secondly, in the algebraical part Abel unnecessarily complicates his proof with a classification of functions according to order and degree. Here he commits an error which caused as acute a mind as Hamilton to declare that "it renders it difficult to judge of the validity of his subsequent reasoning." In this, however, Hamilton was misled, the classification in question being entirely superfluous here, however important in other

*GAUSS, Werke, vol. III. Compare also the interesting paper by Bôcher, BULLETIN, May, 1895.

†Cf. BURKHARDT. Supplement of the *Zeitschrift für Mathematik u. Physik*, vol. 37.

‡ *Oeuvres Complètes*, 2d edition, vol. I., p. 66. It is interesting to compare this with Abel's first attempt which forms the third paper of the new edition.

algebraical investigations. In any case it was highly desirable that a theorem of such far-reaching importance and which stands as it were at the very gateway of any algebraical theory of the roots of higher equations, should be demonstrated in a simple, direct and rigorous manner. Such a demonstration was published by Kronecker in the Monatsberichte* of the Berlin Academy for 1879. This paper has not received the attention of writers of treatises on algebra which it deserves; such standard modern treatises† as Serret, Petersen, Carnoy, all contain demonstrations of the theorem which are imperfect. Serret's demonstration is in its algebraical part almost a word for word reproduction of Abel's memoir and thus contains the unfortunate error noted by Hamilton; the demonstration given by Petersen and Carnoy is vitiated by the same tacit postulate made by Ruffini in the Modena treatise of 1813.

Since the publication of Kronecker's paper in 1879, no other proof has appeared, and yet it seems to me that Kronecker in following Abel too closely in the substitution-theoretical part of his demonstration has not given the simplest proof possible; on the other hand, in the algebraical part, in condensing to the utmost the demonstration, he presupposes that his readers are familiar with the form of proof given by Abel. I propose then in the following lines to give a demonstration of the Ruffini-Abelian Theorem which shall be as direct and *self-contained* as possible; in doing this I hope to render a service to a large class of readers whose studies have led them away from algebraical theories, but who would be glad to see this celebrated theorem demonstrated without implying more or less familiarity with the higher parts of algebra. To aid in this I give at the end of this paper § 8 an illustrative example worked out in detail. In addition to this demonstration I give two others: one, a modification of Ruffini's form; the second, Kronecker's modification of Abel's form. As will be observed, the three forms of demonstration have their algebraical part, essentially due to Abel, in common, while the substitution-theoretical part increases in complexity.

§ 1

We begin by giving a few definitions and establishing one or two elementary theorems.

---

* p. 205 *Vereinfachung des Abel'schen Beweises*, etc.

† SERRET: *Algèbre supérieure* 5th ed. PETERSEN: *Theorie der algebraischen Gleichungen.* CARNOY: *Cours d'Algèbre supérieure.*

We say $f(\lambda, \mu, \nu\cdots)$ is an integral function of the quantities $\lambda, \mu, \nu, \cdots$ when its calculation requires only the operations of addition, subtraction and multiplication in regard to these quantities; every such function is of the type $\Sigma C\lambda^a \mu^b \nu^c \cdots$ where the coefficients C do not involve $\lambda, \mu, \nu\cdots$ and the exponents $a, b, c\cdots$ are positive integers. The function $f(\lambda, \mu, \nu\cdots)$ is said to be a rational function of $\lambda, \mu, \nu\cdots$ when its calculation requires only the operations of addition, subtraction, multiplication and division in regard to them; every such function is the quotient of two integral functions of $\lambda, \mu, \nu\cdots$ and is thus of the type

$$f(\lambda, \mu, \nu\cdots) = \frac{f_1(\lambda, \mu, \nu\cdots)}{f_2(\lambda, \mu, \nu\cdots)}$$

f_1, f_2, being integral. A function $f(a, b, c, \cdots; \lambda, \mu, \nu\cdots)$ may be an integral function in regard to certain quantities $\lambda, \mu, \nu\cdots$ and rational in regard to certain others, $a, b, c\cdots$; if f involves only the quantities $a, b, c\cdots \lambda, \mu, \nu\cdots$ and certain rational numbers, we say $f(a, b, c\cdots \lambda, \mu, \nu\cdots)$ is an integral function of $\lambda, \mu, \nu\cdots$ whose coefficients are rational functions of $a, b, c\cdots$ with rational-number coefficients, or more shortly f is an integral function of $\lambda, \mu, \nu\cdots$ with coefficients rational in $a, b, c\cdots$.

Let $\varphi(\xi, a, b, c\cdots)$ be an integral function of ξ whose coefficients are rational in $a, b, c\cdots$; if $\xi_1, \xi_2, \xi_3\cdots$ be the values of ξ for which $\varphi = 0$,

$$\varphi(\xi) = A(\xi - \xi_1)(\xi - \xi_2)(\xi - \xi_3)\cdots\cdots;$$

similarly if $\eta_1\ \eta_2\ \eta_3\cdots\cdots$ be the zeros of $\psi(\eta, a', b', c'\cdots)$

$$\psi(\eta) = B(\eta - \eta_1)(\eta - \eta_2)(\eta - \eta_3)\cdots\cdots$$

If some of the η's are equal to some of the ξ's as

$$\eta_1 = \xi_1,\ \eta_2 = \xi_2, \cdots\cdots \eta_\mu = \xi_\mu$$

then φ and ψ have a common divisor

$$\delta = (\xi - \xi_1)\cdots(\xi - \xi_\mu)$$

As δ can be obtained by the process of finding the greatest common divisor, and as this process never requires other than rational operations on the coefficients of φ, ψ which are rational in the quantities $a, b, c\cdots a', b', c'$, it follows that δ is an integral function of ξ with coefficients rational in $a, b, c\cdots a', b', c'\cdots$. The function $f(\xi, a, b, c\cdots)$ is said to be irreducible in regard to certain quantities $\lambda, \mu, \nu\cdots$ when it is not the product of factors whose coefficients are rational in $\lambda, \mu, \nu, \cdots$; in the same way the equation $f(\xi) = 0$ is said to

be irreducible under the same circumstances. From this definition it follows that if $f(\xi, a, b, c\cdots)$ be irreducible in regard to $a, b, c\cdots$and certain quantities $\lambda, \mu, \nu\cdots$and have a divisor δ in common with $\varphi(\xi, a, b, c\cdots\lambda, \mu, \nu\cdots)$ then φ is divisible by f. For δ as we saw is of the form $\delta(\xi, a, b, c\cdots\lambda, \mu, \nu\cdots)$; which being a factor common to f and φ, requires that f possess a factor whose coefficients are rational in $a, b, c\cdots\lambda, \mu, \nu\cdots$which is impossible unless $f=\delta$, that is unless φ is divisible by f. Hence:

THEOREM I: If

$$f(\xi, a, b, c\cdots)=\xi^m+A_1\xi^{m-1}+\cdots+A_m=0$$

be irreducible in regard to $a, b, c\cdots\lambda, \mu, \nu\cdots$, and if at the same time ξ satisfy the equation of *less* degree

$$\xi^\mu+B_1\xi^{\mu-1}+\cdots+B_\mu=0 \qquad \mu<m$$

where the B are rational in $a, b, c\cdots\lambda, \mu, \nu\cdots$then

$$B_1=0 \quad B_2=0\cdots\cdots B_\mu=0$$

We turn now to the substitution theory.
The number of permutations of n things

$$1, 2, 3\cdots\cdots n$$

is $n!$; let

$$l_1\ l_2\ l_3\cdots\cdots l_n$$

denote one of these permutations; the operation which replaces 1 by l_1, 2 by $l_2\cdots n$ by l_n is called a substitution and is denoted by the symbol

$$s=\begin{pmatrix} 1 & 2 & 3\cdots n \\ l_1 & l_2 & l_3\cdots l_n \end{pmatrix}$$

where the order of the top row is indifferent if only the l_1 is under 1, l_2 under 2 etc., in each case. As to each of the $n!$ permutations corresponds a substitution, there are $n!$ substitutions affecting the n things $1, 2\cdots n$. I shall speak of them as the substitutions of the symmetric group G or as the substitutions of G. One of these substitutions is

$$\begin{pmatrix} 1 & 2 & 3\cdots n \\ 1 & 2 & 3\cdots n \end{pmatrix}$$

which leaving each element unchanged is called the identical substitution and denoted briefly by 1. Let $s, t, u,\cdots$

be certain substitutions, the operation arising from operating first with s, then with t is denoted by $s.t$ and is called the product of s, t; similarly $s\,t\,u$ is the resulting operation arising from operating first with s, then with t finally with u.

A substitution which replaces each element of the top row by the following, finally the last by the first is called a cycle or a circular substitution; thus

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\quad\begin{pmatrix}4&2&1&5&3\\2&1&5&3&4\end{pmatrix}$$

are such. Every substitution is the product of cycles, thus

$$\begin{pmatrix}1&2&3&4&5&6&7\\3&1&7&5&6&4&2\end{pmatrix}=\begin{pmatrix}1&3&7&2\\3&7&2&1\end{pmatrix}\begin{pmatrix}4&5&6\\5&6&4\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11\\10&8&3&6&7&5&4&9&2&1&11\end{pmatrix}=\begin{pmatrix}1&10\\10&1\end{pmatrix}\begin{pmatrix}2&8&9\\8&9&2\end{pmatrix}\begin{pmatrix}3\\3\end{pmatrix}\begin{pmatrix}4&6&5&7\\6&5&7&4\end{pmatrix}\begin{pmatrix}11\\11\end{pmatrix}$$

A circular substitution of two elements as (12) is a transposition. To every substitution s corresponds *one* substitution t such that $st=1$; thus if

$$s=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$$

the substitution t is

$$t=\begin{pmatrix}4&3&1&2\\1&2&3&4\end{pmatrix}$$

for s converts

$$1\ 2\ 3\ 4$$

into $$4\ 3\ 1\ 2$$

respectively but each element of this last row is converted by t into

$$1\ 2\ 3\ 4$$

respectively, so the joint effect of s and t, or $s.t$ is to leave each element unchanged $\therefore\ st=1$. The substitution t is called the inverse of s and denoted by s^{-1}, so that $s\,s^{-1}=1$. For brevity also we put $s.s=s^2$, $s.s.s=s^3$, etc.

Let $x_1\ x_2\cdots x_n$ be the roots of $x^n+a_1\,x^{n-1}+\cdots+a_n=0$, and let $\varphi\,(x_1, x_2\cdots x_n;\ \lambda,\ \mu,\cdots)$ be a rational function of $x_1\,x_2\cdots x_n$ and certain quantities $\lambda,\ \mu,\cdots$; if φ remain invariant *in form*, however we permute the indices 1, 2, $3\cdots n$, or what is the same thing, for all the substitutions of the symmetric group G, φ is said to be a rational symmetric function of $x_1\,x_2\cdots x_n$.

An elementary theorem of algebra is the following:

THEOREM II. Every rational symmetric function $\varphi(x_1\ x_2,\cdots x_n;\ \lambda,\mu,\nu)$ of the roots $x_1\ x_2\cdots x_n$ of the equation $x^n+a_1x^{n-1}+\cdots+a_n=0$, is a rational function of the coefficients $a_1,\ a_2\cdots a_n$ and the quantities $\lambda,\mu,\nu\cdots$.

The function $f(\lambda,\mu,\nu\cdots.)$ is said to be an explicit algebraical function of $\lambda,\mu,\nu\cdots$when its calculation requires in addition to the rational operations only the extraction of roots in regard to the quantities $\lambda,\mu,\nu\cdots$.

We shall call the equation

$$(a)\qquad f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0$$

general when its coefficients are independent variables, and it shall possess an algebraic solution when their exists an explicit algebraic function of the coefficients which satisfies it. We propose to prove that when n is greater than four, no such function exists by showing that the admission of its existence leads to a contradiction.

§ 2

In fact let us seek the most general form of an explicit algebraical function of the coefficients $a_1\ a_2\cdots a_n$. It may be obtained as Ruffini remarked as follows:

Taking a rational function of the a's as $f_1(a_1\ a_2\cdots a_n)$ we extract a p_1^{th} root; calling this radical R_1 we form a rational function of the a's and of R_1 as $f_2(a_1\cdots a_n, R_1)$ and extract a p_2^{th} root; calling this radical R_2 we form a rational function of the a's and of R_1 and R_2 as $f_3(a_1\ a_2\cdots a_n;\ R_1\ R_2)$, and extract a p_3^{th} root which we call R_3; proceeding in this way every explicit algebraical function x_0 will be defined by the *suite* of equations:

$$(A)\qquad \begin{gathered} R_1^{p_1}=f_1(a_1\ a_2\cdots a_n),\ R_2^{p_2}=f_2(a_1\cdots a_n;\ R_1),\cdots \\ R_\lambda^{p_\lambda}=f_\lambda(a_1a_2\cdots a_n;R_1R_2\cdots R_{\lambda-1}),\ x_0=f(a_1a_2\cdots a_n,R_1,R_2\cdots R_\lambda) \end{gathered}$$

the functions f being all rational in regard to the quantities within the parentheses.

We proceed now to show how the *suite* may be simplified without losing its generality. In the first place the exponents p_k may be taken to be primes, since the extraction of an mn^{th} root may be effected by the extraction of an m^{th}, and from that an n^{th} root. Another simplification arises by observing that no loss of generality is incurred by considering f_k to be an integral function of the radicals $R_1\ R_2\cdots R_{-1k}$ with coefficients rational in $a_1, a_2,\cdots a_n$.

For let for example $f(a_1 \cdots a_n, u)$ be a rational function of u with coefficients rational in $a_1 \cdots a_n$, and

$$u^p = g(a_1 \cdots a_n) \tag{1}$$

then f is of the form

$$f = \frac{b_0 + b_1 u + b_2 u^2 + \cdots + b_{p-1} u^{p-1}}{c_0 + c_1 u + c_2 u^2 + \cdots + c_{p-1} u^{p-1}} = \frac{\varphi(u)}{\psi(u)} \tag{2}$$

the coefficients b, c being rational in the a's. It is to be noticed that neither φ nor ψ contains powers of u higher than $p-1$, since all higher powers may be reduced by observing that

$$u^p = g \quad u^{p+1} = u^p . u = g . u, \quad u^{p+2} = u^p . u^2 = g u^2 \cdots$$

and g is rational in the a's.

The expression (2) may be made integral in regard to u as follows: let the p roots of (1) be

$$u, \quad u_1 = \omega u \quad u_2 = \omega^2 u \cdots u_{p-1} = \omega^{p-1} u$$

where $\omega\, \omega^2 \cdots$ are the roots of the equation

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 = 0 \tag{3}$$

The product

$$P = \psi(u)\, \psi(u_1) \cdots \psi(u_{p-1})$$

is a symmetric function of the roots of (1) and is thus a rational function $P(a_1 \cdots a_n)$ of $a_1 \cdots a_n$; further the product

$$Q = \psi(u_1) \psi(u_2) \cdots \psi(u_{p-1})$$

considered as a function of ω is symmetric in the roots of (3) and is thus an integral function $Q(a_1, \cdots a_n; u)$ of u with coefficients rational in $a_1 \cdots a_n$. We have thus, multiplying numerator and denominator by Q,

$$f = \frac{\varphi Q}{\psi Q} = \frac{\varphi Q}{P};$$

and the right hand member is now an integral function of u with coefficients rational in $a_1 \cdots a_n$. Thus every rational function $f(a_1 \cdots a_n, u)$ can be expressed as an integral function of u, with coefficients rational in $a_1 a_2 \cdots a_n$.

Precisely the same reasoning applies to a rational function $f(a_1 a_2 \cdots a_n, u, v)$ where

$$v^q = h(a_1 \cdots a_n, u) \tag{4}$$

the function h being an integral function of u with coefficients rational in $a_1 a_2 \cdots a_n$. In fact arranging according to ascending power of v

$$f(u, v) = \frac{l_0 + l_1 v + l_2 v^2 \cdots + l_{q-1} v^{q-1}}{m_0 + m_1 v + m_2 v^2 + \cdots + m_{q-1} v^{q-1}} = \frac{\lambda(v)}{\mu(v)}$$

where the coefficients l, m, as rational functions of $a_1 \cdots a_n$, u may be taken as integral functions of u with coefficients rational in $a_1 \cdots a_n$. Making the denominator $\mu(v)$ symmetric in respect to the roots

$$v, v_1, v_2 \cdots\cdots v_{q-1}$$

of (4) by multiplying numerator and denominator by $\mu(v_1) \cdots \mu(v_{q-1})$ we see that

$$f(u, v) = \frac{\lambda(v)\, \mu(v_1) \cdots \mu(v_{q-1})}{\mu(v)\, \mu(v_1) \cdots \mu(v_{q-1})}$$

is an integral function of u, v, with coefficients rational in $a_1 \cdots a_n$. These considerations being applicable to rational functions of any number of radicals, we see that without loss of generality we may assume that the functions f in (A) are integral functions in regard to $R_1 R_2 \cdots$ with coefficients rational in respect to $a_1 a_2 \cdots a_n$.

Finally we observe that we can assume that the equations

$$R_k^{p_k} = f_k \qquad k = 1, 2 \cdots \lambda \tag{5}$$

are irreducible in respect to

$$a_1 \cdots a_n;\ R_1, R_2 \cdots R_{k-1} \tag{6}$$

For if (5) be reducible let

$$(X - R_k)(X - R_k') \cdots (X - R_k^{(\mu-1)}) \tag{7}$$

be a factor rational in respect to the quantities (6), $R_k, R_k' \cdots R_k^{(\mu-1)}$ being roots of (5); then the absolute term of (7) or

$$R_k R_k' \cdots R_k^{(\mu-1)} = \omega R_k^{\mu}, \qquad \omega^{p_k} = 1$$

is rational in (6), or if λ satisfy $\lambda \mu \equiv 1 \bmod p_k$, $\omega^{\lambda} R_k$ is rational in (6); that is R_k is rational in ω and the quantities (6). But as the determination of ω, as is well known, depends upon the solution of a *suite* of binomial equations whose degrees are the prime factors of $p_k - 1$, the assumption that the equations of the *suite* (A) are irreducible in the above sense, involves no loss of generality.

Thus to sum up: every explicit algebraical function of $a_1\ a_2 \cdots\ a_n$ is represented by the *suite* (A) where f_k is an integral function of the radicals $R_1, R_2 \cdots R_{k-1}$ whose coefficients are rational in $a_1\ a_2 \cdots\ a_n$; the equations $R_k^{p_k} = f_k$ are irreducible in respect to $a_1 \cdots\ a_n$; $R_1 \cdots\ R_{k-1}$; the exponents p_k are primes, finally

$$(b) \qquad x_0 = \Sigma A_k R_\lambda^k \qquad k=0, 1 \cdots p_\lambda - 1$$

where A_k is an integral function of $R_1 \cdots\ R_{\lambda-1}$, with coefficients rational in $a_1 \cdots\ a_n$.

§ 3

We impose now the condition that the explicit algebraical function x_0 shall satisfy the equation (a); this will give us a relation between the roots $x_0\ x_1 \cdots$ and the radical R_λ which will indicate a method of simplifying the suite (A) still further. Raising x_0 to the various powers, and substituting these values of $x_0, x_0^2, x_0^3, \cdots x_0^n$ in (a), we have the equation.

$$(1) \qquad 0 = B_0 + B_1 R_\lambda + B_2 R_\lambda^2 + \cdots + B_{p_\lambda - 1}\ R_\lambda^{p_\lambda - 1}$$

and making use of

$$(2) \qquad R_\lambda^{p_\lambda} = f_\lambda$$

to reduce powers of R_λ higher than $p_{\lambda-1}$; the coefficients B are rational in

$$a_0\, a_1 \cdots a_n,\ R_1, R_2 \cdots,\ R_{\lambda-1}$$

and hence by theorem I., the coefficients B all vanish.* Thus (1) is satisfied when we replace R_λ by αR_λ where $\alpha^{p_\lambda} = 1$. Hence the expressions obtained from (b) when we replace there R_λ by $\alpha^k R_\lambda$, that is

$$(3) \qquad x_k = \Sigma A_k \alpha^{hk} R_\lambda^k \qquad k=0, 1 \cdots p_\lambda - 1$$

satisfy (1) and are thus roots of (a). Here all the coefficients A cannot vanish, let A_k be one of these; if we multiply both sides of the p_λ equations (3) respectively by α^{-k}, $\alpha^{-2k} \cdots \alpha^{-(p_\lambda - 1)k}$, and add, we get, remembering that

$$1 + \alpha^r + \alpha^{2r} + \cdots + \alpha^{(p_\lambda - 1)r} = 0$$

the equation

$$(4) \qquad \Sigma' \alpha^{-hk} x_k = p_\lambda A_k R_\lambda^k$$

which gives us the relation in question.

*We have assumed the *suite* to embrace only irreducible equations; in practice it is convenient to defer the elimination of reducible elements till this stage where we have the means of deciding concerning reducibility.

This relation shows us how we may express x_0 as an integral function of certain radicals

$$P_1, P_2 \cdots P_\lambda$$

where these radicals enjoy the peculiar property of being integral functions of $x_0 x_1 \cdots x_{n-1}$ and certain roots of unity $\alpha, \beta \cdots \omega$ with rational-number coefficients. In fact put†

$$P_\lambda = p_\lambda A_\lambda R_\lambda^h; \tag{5}$$

this equation together with (2) shows that R_λ is a rational function of P_λ and the quantities $R_1, \cdots R_{\lambda-1}$, since the assumption that (2) is irreducible in respect to $R_1 \cdots R_{\lambda-1}$ P_λ is, on account of (3) inadmissible. (Theorem I). As R_λ is rational in respect to these quantities so is x_0. That P_λ satisfies a binomial equation of the type

$$P_\lambda^p = g_\lambda (a_1 \cdots a_n, R_1 R_2 \cdots R_{\lambda-1})$$

is evident; for

$$P_\lambda^p = p_\lambda^p A_\lambda^p R_\lambda^{h^p} = p_\lambda^p A_\lambda^p f_\lambda^h$$

which is a rational function of $a_1 \cdots a_n$ $R_1 \cdots R_{\lambda-1}$ which we denote by g_λ.

The radical R_λ being replaced by P_λ, we proceed now to show how we may replace $R_{\lambda-1}$ by $P_{\lambda-1}$. Put

$$\xi_0 = P_\lambda^p = (\Sigma \alpha^{-h} x_h)^p$$

and let $\xi_0 \xi_1 \xi_2 \cdots$ be the $n!$ functions (different or not) arising from applying the $n!$ substitutions of the symmetric group to ξ_0. Form now the equation

$$\Phi(\xi) = (\xi - \xi_0)(\xi - \xi_1) \cdots = 0,$$

its coefficients being symmetric in $x_0, x_1, \cdots x_n$ are rational in the coefficients $a_1 \cdots a_n$.

Now a moment's reflection shows that the reasoning applied to the equations

$$f(x) = 0, \qquad x_0 = f_\lambda (a_1 \cdots a_n;\ R_1 \cdots R_\lambda)$$

† This step could obviously be omitted if for $h = 1$, A_h is a rational number.

can be applied word for word to the equations

$$\Phi(\xi)=0, \qquad \xi_0=g_\lambda(a_1\cdots a_n;\ R_1\cdots R_{\lambda-1})$$

In fact referring to the reasoning just made in regard to x_0, R_λ we see that we may write

$$(b') \qquad \xi_0=\Sigma A_r' R_{\lambda-1}^r \qquad r=0,1\cdots p_{\lambda-1}-1.$$

which is the equation analogous to (b).

This value of ξ_0 substituted in $\Phi=0$ gives

$$(1') \qquad 0=B_0'+B_1'R_{\lambda-1}+\cdots B'_{p_{\lambda-1}-1}R_{\lambda-1}^{p_{\lambda-1}-1}$$

which is analagous to (1). This shows that the quantities

$$(3') \qquad \xi_s=\Sigma A_r'\beta^{rs}R_{\lambda-1}^r \qquad s=0,1\cdots p_{\lambda-1}-1, \qquad \beta^{p_{\lambda-1}}=1$$

also satisfy $\Phi=0$. These equations now give as before the relation

$$(4') \qquad \Sigma\beta^{-rs}x_s=p_{\lambda-1}A_r'R_{\lambda-1}^r$$

analogous to (4). It follows thus, if we put

$$P_{\lambda-1}=p_{\lambda-1}A_r'R_{\lambda-1}^r$$

that $R_{\lambda-1}$ is a rational function of $R_1, R_2,\cdots R_{\lambda-2}$ and $P_{\lambda-1}$ while on the one hand $P_{\lambda-1}$ satisfies a binomial equation of the type

$$P_{\lambda-1}^{p_{\lambda-1}}=g_{\lambda-1}(a_1\cdots a_n;\ R_1, R_2, R_{\lambda-2})$$

and on the other is an integral function of $\xi_0\ \xi_1\cdots$and β. But $\xi_0\ \xi_1\cdots$are integral functions of $x_0\ x_1\cdots$and α, hence $P_{\lambda-1}$ is an integral function of $x_0\ x_1\cdots x_{n-1}$ and the roots of unity α, β; the coefficients of these functions being rational numbers. Returning now to the expression for x_0, namely:

$$x_0=f(a_1\cdots a_n, R_1\cdots R_{\lambda-1}, R_\lambda),$$

we see that we are in the position to replace the radicals $R_{\lambda-1}$, R_λ by the radicals $P_{\lambda-1}$, P_λ. The same reasoning being applicable to the remaining radicals we have the following:

THEOREM III. If an equation is algebraically solvable, we can always give the explicit algebraic expression for a root such a form that all the radicals entering it are integral functions of the roots $x_0\ x_1\cdots x_{n-1}$ and certain roots of unity $\alpha, \beta,\cdots\omega$, the coefficients of these functions being rational numbers;

the radicals themselves are determined by a *suite* of binomial equations

$$(B) \qquad P_1^{p_1} = g_1(a_1 \cdots a_n) P_2^{p_2} = g_2(a_1 \cdots a_n;\ P_1) \cdots\cdots P_\lambda^{p_\lambda} = g_\lambda(a_1 \cdots a_n; P_1\ P_2 \cdots P_{\lambda-1})$$

while x_0 is given by

$$(C) \qquad x_0 = g(a_1 \cdots a_n;\ P_1\ P_2 \cdots P_\lambda),$$

the functions g being integral functions of $P_1 \cdots\cdots P_\lambda$ with coefficients rational in $a_1 \cdots a_n$.

§ 4.

The theorem just proved affords us a sure foundation to construct the substitution-theoretical part of the demonstration; we give first a form due to Ruffini.* Consider the rational integral function of the roots†

$$\varphi(x_1\ x_2 \cdots x_n)$$

defined by the first equation of (B); let $\varphi_s\ \varphi_{s^2} \cdots\cdots$ be the values of φ after application of $s\ s^2 \cdots$ where

$$s = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix},$$

then since $g_1(a_1 \cdots a_n)$ is a symmetric function of the roots it remains unchanged for s. Applying then s to the identity

$$\varphi^{p_1} = g_1(a_1 \cdots a_n)$$

it becomes $\varphi_s^{p_1} = g_1$ whence

$$(1) \qquad \varphi_s = \beta\varphi \quad \text{where } \beta^{p_1} = 1$$

Applying s to the identity (1) it becomes

$$\varphi_{s^2} = \beta\varphi_s = \beta^2\varphi$$

similarly $\varphi_{s^3} = \beta^3\varphi$, $\varphi_{s^4} = \beta^4\varphi$ and $\varphi_{s^5} = \beta^5\varphi$; but as $s^5 = 1$, $\varphi_{s^5} = \varphi$ and $\beta^5 = 1$.

In the same way, if

$$\sigma = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}$$

*Cf. my paper in *Monatshefte für Mathematik und Physik*, vol. 6, for fuller information concerning this form of proof used by Ruffini in the Modena work already referred to.

† We designate these now by the indices 1, 2...n, as more convenient.

$\varphi_\sigma=\gamma\varphi$ where, as $\sigma^3=1$, $\gamma^3=1$

Hence the application of σ to the identity (1) gives

$$\varphi_{s\sigma}=\beta\varphi_\sigma=\beta\gamma\varphi$$

whence we conclude as above that $(\beta\gamma)^5=1$ since $(s\sigma)^5=1$. Similarly if

$$\rho=\begin{pmatrix}3&4&5\\4&5&3\end{pmatrix}$$

then $\varphi_\rho=\varphi_{\rho^2}=\varphi$; but since $\rho\sigma=s$, $\varphi_{\rho\sigma}=\varphi_s=\varphi$; hence $\beta=1$ since $\varphi_s=\beta\varphi$. That is φ remains not only unaltered for σ and ρ, but also for s. Consider now the rational function of the roots

$$\psi(x_1x_2\cdots x_n)$$

defined by the second equation of the *suite B*. The right hand side of the identity

$$\psi^{p_2}=g_2(a_1\cdots a_n;\ \varphi)$$

remaining unaltered for the substitutions s, σ, ρ we can reason in regard to ψ precisely as we did concerning φ: hence ψ is unchanged for these substitutions. Proceeding in this way we see that all the radicals $P_1\ P_2\cdots P_\lambda$ remain unaltered for s; but applying s to the identical relation (C) viz:

$$x_1=g(a_1\cdots a_n;\ P_1P_2\cdots P_\lambda)$$

we observe that the right hand side remains unaltered whereas the left hand side does not which is an absurdity. The assumption that there exist an explicit algebraical function of the coefficients $a_1\ a_2\cdots a_n$ which satisfies (A), leads thus to a contradiction.

§ 5

An interresting modification of Ruffini's proof is the following: We just saw that P_ν $(\nu=1, 2)$ remain unaltered by the circular substitution $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$; as the indices 1,2,3,4,5 employed in showing this were any five of the n indices, it follows that P_ν remain unaltered for every circular substitution of three indices. These substitutions we shall call the substitutions of the alternate group which we denote shortly by Γ. We propose to show that P_ν remain unaltered

for no other substitutions of the symmetric group G; having established this it follows that the radical P_2 is rational in P_1 which violates the hypothesis made in regard to the *suite B*. In the first place P_1 must change its value for every transposition $\tau=(\lambda, \mu)$ for if it remain unaltered for *any* transposition we show that it remains unaltered for *every* transposition; as every substitution is the product of cycles and as $\begin{pmatrix} 1\,2\,3\cdots m \\ 2\,3\,4\cdots 1 \end{pmatrix}$ is the product of transpositions $(12)(13)\cdots(1\,m)$, P_1 would remain unaltered for every substitution, and then being symmetric functions of the roots, it would be rational in $a_1\, a_2 \cdots a_n$.

Suppose then P_1 remain unaltered for τ, let λ be any substitution of G, then P_1 remains unaltered for $\varphi=\lambda^{-1}\tau\lambda$; for since $P_{\lambda^{-1}\tau}=P_{\lambda^{-1}}$ we have $P_{\lambda^{-1}\tau\lambda}=P_{\lambda^{-1}\lambda}=P_1$

Now, by properly choosing λ, ρ can represent any transposition $(l_\lambda\, l_\mu)$; for let

$$\lambda=\begin{pmatrix} 1 & 2 & 3\cdots n \\ l_1 & l_2 & l_3\cdots l_n \end{pmatrix}$$

then λ^{-1} converts

(1) $$l_1\, l_2\, l_3\cdots l_\lambda\cdots l_\mu\cdots l_n$$

respectively into

$$1\,2\,3\cdots\lambda,\cdots\mu\cdots n$$

which τ converts respectively into

$$1\,2\,3\cdots\mu\cdots\lambda\cdots n$$

which finally λ converts into

(2) $$l_1\, l_2\, l_3\cdots l_\mu\cdots l_\lambda\cdots l_n\,;$$

that is the substitution $\rho=\lambda^{-1}\tau\lambda$ converts (1) into (2) so that ρ leaving every index except l_λ, l_μ unaltered and merely transposing these

$$\rho=(l_\lambda, l_\mu)$$

Thus every transposition alters P_1; but every pair of transpositions leaves it unchanged, since every such pair is of the type

$$(1\,2)\ (3\,4) \quad \text{or} \quad (1\,2)\ (2\,3),$$

but the first being equal to $\begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}\begin{pmatrix} 3\,1\,4 \\ 1\,4\,3 \end{pmatrix}$ and the second equal to $\begin{pmatrix} 1\,3\,2 \\ 3\,2\,1 \end{pmatrix}$, both are substitutions of Γ. From this we

conclude that if any substitution s be the product of m transpositions, it will alter or leave unaltered the radical P_1 according as m is odd or even. This shows that however s be decomposed into a product of transpositions, their number is always odd or always even, and we say s is an odd or even substitution according as m is. As I' contains all the even substitutions of G, P_1 and hence P_2 also is altered for every substitution not in I'. The number of substitutions I' in G is $\frac{1}{2}\,n\,!$; for let

$$(1) \qquad s_1=1,\ s_2,\ s_3\cdots s_m$$

be the even substitution, and

$$t_1\ t_2\ t_3\cdots t_\mu$$

be the odd; then,

$$(2) \qquad t_1, s_2t_1, \cdots\cdots s_m\ t_1$$

are distinct and odd, hence $\mu \geqq m$; also

$$t_1\cdot t_1,\ t_2t_1,\ t_3t_1, \cdots t_\mu\ t_1$$

are distinct and even, hence $m \geqq \mu$ $\therefore$ $m=\mu=\frac{1}{2}\,n\,!$ This shows that P_ν acquire but two values for the substitutions of G; for they remain unchanged for (1) while they both change for the substitutions (2) into P_ν', and there are no other substitutions in G.

We now conclude easily that P_2 is rational in P_1. As P_1 is root of a binominal equation, it follows that $P_1'=-P_1$; also the coefficients of

$$\Phi(x)=(P_2+P_2')\,x+P_1\,(P_2-P_2')$$

being unaltered for the substitutions of G, are rational in $a_1\ a_2\cdots a_n$; denotingthem by A, B, we have

$$\Phi(x)=Ax+B$$

But $$\Phi(P_1)=A\,P_1+B=2\,P_1\,P_2,$$

hence $$P_2=\frac{A\,P_1+B}{2\,P_1}$$

and P_2 is rational in P_1 and the coefficients $a_1\cdots a_n$.

§ 6.*

We turn now to Kronecker's form of Abel's proof. From the preceding paragraph we take as proven that P_1 is un-

* In anticipation of questions of priority, I remark that this paragraph formed part of a paper I had the honor to read before the Yale Mathematical Club, December 4, 1894. No changes except of the most insignificant nature have been made in the text.

altered for the substitution of Γ, and that every rational function of the roots unaltered for Γ is rational in P_1. Consider the rational function of the roots $\psi(x_1 x_2 \cdots x_n) = P_2$ defined by the second equation of the *suite* (B)

$$\psi^{p_2} = g_2(P_1). \tag{1}$$

The $\frac{1}{2}n!$ functions (different or not)

$$\psi\, \psi_1\, \psi_2 \cdots\cdots \tag{2}$$

which arise from ψ on applying to it the $\frac{1}{2}n!$ substitution of Γ must all be of the form

$$\omega\psi, \qquad \omega^{p_2} = 1$$

since the right hand side of (1) remains unaltered for these substitutions. Thus if ψ remain unaltered for one substitution

$$\sigma = \begin{pmatrix} 1, 2, 3 \cdots n \\ l_1\, l_2\, l_3 \cdots l_n \end{pmatrix}$$

of Γ besides the identical substitution, all the conjugate functions (2) must also remain unaltered for σ. But such a substitution must exist since $\frac{1}{2}n! > p_2$; in fact the coefficients of the equation

$$\Phi(x) = (x-\psi)(x-\psi_1)(x-\psi_2)\cdots \tag{3}$$

being symmetric in (2) are unchanged for the substitutions of Γ and are thus rational in P_1.

But $\Phi = 0$ having the root $x = \psi$ in common with the irreducible equation

$$P_2^{p_2} = g_2(P_1) \tag{4}$$

is satisfied by all the roots of (4) and hence $\frac{1}{2}n! \equiv p_2$; as p_2 is prime $\frac{1}{2}n! > p_2$.

We now show that the conjugate functions (2) remaining unaltered by σ a substitution different from the identical substitution, remain unaltered for every substitution

$s = \begin{pmatrix} 1 & 2 \cdots n \\ h_1 & h_2 \cdots h_n \end{pmatrix}$ of Γ and $P_2 = \psi$ is thus rational in P_1 which

is contrary to hypothesis. To do this Kronecker remarks that ψ remains unaltered for every substitution ρ of Γ which changes

$$l_{h_k} \text{ into } h_{l_k} \qquad k = 1, 2 \cdots n$$

In fact $\rho=\sigma^{-1}s^{-1}\sigma s$, for σ^{-1} changes l_{h_k} into h_k which s^{-1} changes into k which is changed by σ into l_k which finally s changes into h_{l_k}. But that $\psi_\rho=\psi$ is manifest since by hypothesis $\psi_\sigma=\psi$ and hence $\psi_{\sigma^{-1}}=\psi$ also, but then $\psi_{\sigma^{-1}s^{-1}}=\psi_{s^{-1}}$ and $\psi_{\sigma^{-1}s^{-1}\sigma}=\psi_{s^{-1}\sigma}=\psi_{s^{-1}}$, hence finally $\psi_{\sigma^{-1}s^{-1}\sigma s}=\psi_{s^{-1}s}=\psi$. Thus if ψ remain unaltered for σ it also remains unaltered for ρ; which enables us to show that ψ is unchanged for at least one circular substitution of three elements. For whatever σ may be it is of one of the five following types:

1° σ contains at least one cycle of more than three letters and is of the form

$$\sigma_1=\begin{pmatrix}1&2&3&\cdots&m\\2&3&4&\cdots&1\end{pmatrix}c_1c_2\cdots\cdots$$

where $c_1c_2\cdots$ denote other cycles of σ_1

2° it contains two or more cycles of three elements, but no cycle of more elements, and

$$\sigma_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}4&5&6\\5&6&4\end{pmatrix}c_1c_2\cdots$$

3° it contains only one cycle of three elements and one or more transpositions

$$\sigma_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}4&5\\5&4\end{pmatrix}c_1c_2\cdots$$

4° it contains only transpositions, but of these at least three

$$\sigma_4=(1\,2)\,(3\,4)\,(5\,6)\,c_1c_2\cdots$$

5° it contains only two transpositions

$$\sigma_5=(1\,2)\,(3\,4)\,(5)\cdots$$

Put now $\rho_\lambda=\sigma_\lambda^{-1}\sigma_\lambda^{-1}\sigma_\lambda s_\lambda$

$$s_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad s_2=\begin{pmatrix}1&4&5\\5&4&1\end{pmatrix}\quad s_3=\begin{pmatrix}1&2&4\\2&4&1\end{pmatrix}\quad s_4=\begin{pmatrix}1&3&5\\3&5&1\end{pmatrix}=s_5$$

then

$$\rho_1=\begin{pmatrix}1&2&4\\2&4&1\end{pmatrix}\quad \rho_2=\begin{pmatrix}1&4&5&2&6\\4&5&2&6&1\end{pmatrix}\quad \rho_3=\begin{pmatrix}1&2&5&3&4\\2&5&3&4&1\end{pmatrix}$$

$$\rho_4=\begin{pmatrix}1&3&5\\3&5&1\end{pmatrix}\begin{pmatrix}2&6&4\\6&4&2\end{pmatrix},\quad \rho_5=\begin{pmatrix}1&3&5&4&2\\3&5&4&2&1\end{pmatrix}$$

which shows that all the cases may be reduced to 1°. Hence ψ remains unaltered for some circular substitution of three elements

$$\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

But if ψ remain unchanged for τ it will also remain invariant for

$$(5)\qquad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&4\\2&4&1\end{pmatrix},\ \begin{pmatrix}1&2&5\\2&5&1\end{pmatrix},\ \cdots\begin{pmatrix}1&2&n\\n&2&1\end{pmatrix}$$

For let $t=\begin{pmatrix}1&2&\nu\\2&\nu&1\end{pmatrix}$, then ψ being invariant for τ is for $t^{-1}\tau t^{-1}=\omega$ and hence for ω; but $\omega=\begin{pmatrix}2&\nu&3\\\nu&3&2\end{pmatrix}$ and hence

$$\omega^2=\begin{pmatrix}2&3&\nu\\3&\nu&2\end{pmatrix}\qquad\qquad \nu=4,5\cdots n$$

Every substitution of Γ is the product of the substitutions of (5), for every substitution of Γ is the product of a certain number of pairs of transpositions

$$(1\,2)\quad(1\,3)\quad\cdots(1\,n).$$

Let $(1\lambda)\,(1\mu)$ be such a pair, then as

$$(1\lambda)\,(1\mu)=\begin{pmatrix}1&2&\lambda\\2&\lambda&1\end{pmatrix}\begin{pmatrix}1&2&\lambda\\2&\lambda&1\end{pmatrix}\begin{pmatrix}1&2&\mu\\\mu&2&1\end{pmatrix}$$

ψ remains unaltered for every substitution of Γ.

This demonstration, while longer than either of the two preceding ones, is interesting from a historical view, as the lemma on the conjugate functions ψ contains as a corollary Cauchy's theorem, which is fundamental in Abel's proof. In fact let

$$\varphi_1\quad\varphi_2\quad\cdots\varphi_m$$

be the m distinct values which a rational function φ of $x_1 x_2\cdots x_n$ assumes for the substitutions of Γ; as no substitution of Γ leaves *all* the φ's unchanged every substitution of Γ will give rise to a permutation of the above m indices; as there are only $m!$ permutation of m things this number must be certainly as great as $\frac{1}{2}n!$ and

$$m!\geq\tfrac{1}{2}n!$$

Now if $m < n$ then not only is $m! < n!$ but also $m! < \frac{1}{2} n!$ which is impossible. Thus every rational function φ of $x_1 x_2 \cdots x_n$ which takes on more than two values, takes on at least n values; which is Cauchy's theorem.

§ 7.

It being demonstrated that the general equation of degree $n > 4$ possesses no algebraic solution when the coefficients are regarded as independent variables, it lies very near to inquire whether there are equations with constant coefficients, say with rational-number coefficients, which do not possess an algebraic solution. To this very important question the Ruffini-Abelian theorem gives no reply; however in looking over the reasoning employed in the last three paragraphs we observe that its correctness depends upon the obvious fact that every rational equation

$$\Phi(x_1 x_2 \cdots x_n\, \alpha, \beta \cdots) = 0 \tag{1}$$

between the roots and certain roots of unity $\alpha, \beta \cdots$, the coefficients being rational numbers, remains true on applying to it any substitution of the alternate group Γ. The question is thus reduced to this: do there exist equations of every degree, whose coefficients are rational numbers such that every relation (1) still subsists on applying any substitution of Γ? That this is so has been shown by Hilbert.* Hence not only has the *general* equation of degree > 4 no algebraic solution, but there exists an infinity of equations of every degree with integral coefficients which possess this property.

§ 8.

We close by giving an illustration of §§ 2, 3 applied to the explicit algebraic function

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

root of the cubic

$$x^3 + px + q = 0 \tag{1}$$

Here

$$R_1^3 = f_1(p, q) = \frac{q^2}{4} + \frac{p^3}{27};\quad R_2^3 = f_2(p, q, R_1) = -\frac{q}{2} + R_1$$

$$R_3^3 = f_3(p, q, R_1, R_2) = -\frac{q}{2} + R_1 \tag{a}$$

$$x_0 = R_2 + R_3 \tag{2}$$

* CRELLE, vol. 110, p. 104.

We proceed to replace the *suite* (α) by a *suite* (β) of the type (B) of § 3. Raising (2) to the 2nd and 3rd powers and substituting in (1) we get

$$R_3^3 + 3\,R_2\,R_3^2 + (3\,R_2^2 + p)\,R_3 + (R_2^3 + p\,R_2 + q) = 0$$

or reducing by aid of

$$R_3^3 = f_3 = -\frac{q}{2} - R_1 \qquad R_2^3 = -\frac{q}{2} + R_2$$

we get

$$3\,R_2 . R_3^2 + (3\,R_2^2 + p)\,R_3 + p\,R_2 = 0$$

As the coefficients of this equation are not zero, the last equation of (α) cannot be reducible and R_3 must be rational in the preceding radicals. In fact we know that

$$R_3 = -\frac{p}{3\,R_2}$$

Equation (2) becomes thus

$$x_0 = R_2 - \frac{{}^1/_3\,p}{R_1 - \frac{1}{2}\,q}\,R_2^2 \tag{3}$$

The denominator here is $-R_1 - \frac{1}{2}\,q$ whose conjugate value is $-R_1 - \frac{1}{2}\,q$; hence multiplying numerator and denominator of the second term of the right member of (3) by this last, (3) becomes

$$x_0 = R_2 - \frac{9}{p^2}(R_1 + \tfrac{1}{2}\,q)\,R_2^2 \tag{4}$$

which is an integral function of R_1, R_2 with coefficients rational in p, q. The value of x_0 given by (4) substituted in (1) gives

$$0 = B_0 + B_1\,R_2 + B_2 R_2^2,$$

where

$$B_0 = R_1 - \frac{q}{2} - \frac{3^6}{p^6} \cdot \frac{p^6}{3^6}(R_1 + \tfrac{1}{2}\,q)$$

$$B_1 = -\frac{3^3}{p^2}\frac{p^3}{3^3} + p$$

$$B_2 = \frac{3^5}{p^4}\,\frac{p^3}{3^3}\,(_1 + \tfrac{1}{2}\,q) - \frac{3^2}{p}\left(R_1 + \frac{q}{2}\right)$$

which are all identically equal to zero. Hence not only is (4) a root of (1) but so also are the quantities which we

deduce from it in replacing R_2 by ωR_2 and $\omega^2 R_2$ ($\omega^3 = 1$). Denoting these roots respectively by $x_0\, x_1\, x_2$ we have

$$x_0 = R_2 - \frac{3^2}{p^2}(R_1 + \tfrac{1}{2}q)\, R_2^2$$

$$x_1 = \omega R_2 - \frac{3^3}{p^2}(R_1 + \tfrac{1}{2}q)\omega^2 R_2^2$$

$$x_2 = \omega^2 R_2 - \frac{3^2}{p^2}(R_1 + \tfrac{1}{2}q)\omega R_2^2$$

As the coefficient of R_2 is here 1 we do not need to replace R_2 by a new radical. Solving we get

$$R_2 = \tfrac{1}{3}\Sigma\omega^{-k} x_k \qquad k = 0, 1, 2$$
$$= \frac{x_0 + \omega^2 x_1 + \omega x_2}{3}$$

The suite (α) is now replaced by

$$R_1^2 = f_1 \quad R_2^3 = f_2$$
$$(\beta) \qquad x_0 = g(p, q, R_1, R_2)$$
$$= R_2 - \frac{9}{p^2}(R_1 + \tfrac{1}{2}q)\, R_2^2$$

and the first step has been accomplished.

We have now to reason in the same way in regard to the remaining radical R_1. To this end we form the equation $\varphi(\xi) = 0$ whose roots are the values of

$$\xi_0 = R_2^3 = \left(\frac{x_0 + \omega^2 x_1 + \omega x_2}{3}\right)^3$$

As ξ_0 acquires only two distinct values, Φ will be the cube of an integral function of ξ with coefficients rational in p, q; this is easily found to be

$$\varphi(\xi) = \xi^2 + q\xi - \tfrac{1}{27}p^3,$$

Substituting here the value of ξ given in (β), $\varphi(\xi) = 0$ becomes

$$(R_1 - \tfrac{q}{2})^2 + q(R_1 - \tfrac{q}{2}) - \tfrac{1}{27}p^3 = 0,$$

or

$$B_0 + B_1 R_1 = 0$$

where

$$B_0 = \tfrac{1}{4}q^2 + \tfrac{1}{4}q^2 - \tfrac{1}{2}q^2 + \tfrac{1}{27}p^3 - \tfrac{1}{27}p^3$$
$$B_1 = q - q$$

vanish identically; whence not only

$$\xi_0 = R_1 - \frac{q}{2}$$

but also

$$\xi_1 = -R_1 - \frac{q}{2}$$

is a root of $\varphi = 0$.

Whence

$$R_1 = \tfrac{1}{2}(\xi_0 - \xi_1) = \tfrac{1}{2 \cdot 3^3}\left[(x_0 + \omega^2 x_1 + \omega x_2)^3 - (x_0 + \omega x_1 + \omega^2 x_2)^3\right]$$

$$= -\frac{\sqrt{-3}}{2.9}\sqrt{\Delta},$$

where $\Delta = (x_0 - x_1)^2 (x_1 - x_2)^2 (x_1 - x_2)^2$ is the discriminant of (1). Thus the *suite* (β) has the character (B).

YALE UNIVERSITY,
NEW HAVEN, CONN.

ON CERTAIN SUB-GROUPS OF THE GENERAL PROJECTIVE GROUP.

BY PROFESSOR HENRY TABER.

[Read at the January meeting of the Society, 1896.]

§ 1

In what follows a linear transformation homogeneous in n variables as

$$\begin{aligned} x_1' &= a_{11} x_1 + a_{12} x_2 + \cdots + a_{1n} x_n, \\ x_2' &= a_{21} x_1 + a_{22} x_2 + \cdots + a_{2n} x_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_n' &= a_{n1} x_1 + a_{n2} x_2 + \cdots + a_{nn} x_n, \end{aligned}$$

will be denoted by the single letter A. If x_1, x_2, etc., are the Cartesian coördinates of a point in n-fold space, the transformation A is a homogeneous strain; and the totality of transformations A constitutes the group of homogeneous strains in n-fold space. If we consider only transformations A of non-zero determinant, we obtain Lie's *general linear homogeneous group*. The group of transformations A of determinant $+1$ is termed by Lie the *special linear homogeneous group*.

If B denotes the transformation

$$x_r'' = b_{r1} x_1' + b_{r2} x_2' + \cdots + b_{rn} x_n' \ (r=1, 2, \cdots n),$$

the transformation resulting from the successive application to n-fold space of A and B (in the order named), defined by the system of equations

$$x_r'' = \sum_1^n{}_i b_{ri} a_{i1} \quad x_1 + \sum_1^n{}_i b_{ri} a_{i2} \cdot \ x_2 + \cdots + \sum_1^n{}_i b_{ri} a_{in} \cdot x_n$$

$$(r=1, 2, \cdots n),$$

will be denoted by BA.

If the transformation B is identical with A, this may be indicated by writing $B=A$; and in this case the transformation $BA=BB$ may be denoted by B^2. Similarly the transformation resulting from the repetition $m-1$ times of the transformation B (that is, the transformation resulting from m successive applications of B) may be denoted by B^m, which may be termed the m^{th} *power* of B.

If for $r, s = 1, 2, \cdots n$,

$$b_{rr} = 1, \ b_{rs} = 0 \ (r \neq s),$$

B is the *identical transformation*. The letter I will be employed to denote the identical transformation. We have $IA = AI = A$. We may denote the transformation for which

$$b_{rr} = \rho, \ b_{rs} = 0 \ (r \neq s),$$

by ρI; and the transformation $\rho I. A$, defined by the equations $x_r' = \rho a_{r1} x_1 + \rho a_{r2} x_2 + \cdots + \rho a_{rn} x_n \ (r = 1, 2, \cdots n)$ may be denoted simply by ρA. In particular, the transformation defined by the equations

$x_r' = -a_{r1} x_1 - a_{r2} x_2 - \cdots - a_{rn} x_n \ (r = 1, 2, \cdots n)$ will be denoted by $-A$.

The transformation B is *infinitesimal* if

$$b_{rr} = 1 + c_{rr} \delta t, \quad b_{rs} = c_{rs} \delta t \quad (r \neq s),$$

where c_{rr} and c_{rs} are constants, and δt is an infinitesimal quantity.

Following Sylvester, I shall say that the nullity of B is m if the minor determinants of order $n-m+1$ of the matrix

$$\left\| \begin{matrix} b_{11}, & b_{12}, & \cdots\cdots & b_{1n} \\ b_{21}, & b_{22}, & \cdots\cdots & b_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ b_{n1}, & b_{n2}, & \cdots\cdots & b_{nn} \end{matrix} \right\|$$

are all zero, but not all the minors of order $n-m$.

If we denote by A_λ the transformation

$$\begin{aligned} x_1' &= (a_{11}-\lambda)\, x_1 + a_{12}\, x_2 + \cdots a_{1n}\, x_n, \\ x_2' &= a_{21}\, x_1 + (a_{22}-\lambda)\, x_2 + \cdots + a_{2n}\, x_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_n' &= a_{n1}\, x_1 + a_{n2}\, x_2 + \cdots + (a_{nn}-\lambda)\, x_n, \end{aligned}$$

where λ is a root of multiplicity μ of the *characteristic equation* of A,

$$\left| \begin{matrix} a_{11}-z, & a_{12}, & \cdots\cdots & a_{1n} \\ a_{12}, & a_{22}-z & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1}, & a_{n2}, & \cdots\cdots & a_{nn}-z \end{matrix} \right| = 0,$$

the nullity of A_λ is at least one, and cannot exceed μ. If the nullity of A_λ is equal to μ, the nullity of A_λ^2, A_λ^3, etc., is also μ. On the other hand, if the nullity of A_λ is less than μ, the nullity of A_λ^2 is greater by one, at least, than the nullity of A_λ; and the nullity of successive powers of A_λ increases until a power of exponent ν is attained whose nullity is μ. The nullity of the $(\nu+1)^{th}$ and higher powers of A_λ is then also μ. If we denote by

$$\mu_1, \mu_2, \cdots \mu_{\nu-1}, \mu_\nu = \mu,$$

respectively, the nullities of

$$A_\lambda, A_\lambda^2, \cdots A_\lambda^{\nu-1} A_\lambda^\nu,$$

we have

$$\mu_1 \geqq \mu_2 - \mu_1 \geqq \mu_3 - \mu_2 \geqq \cdots \geqq \mu_\nu - \mu_{\nu-1} \geqq 1.$$

I shall term the numbers $\mu_1, \mu_2 \cdots \mu_\nu$ the numbers *belonging* to the root λ of the characteristic equation A. We can always find a transformation A which shall have any complex number λ as a root of its characteristic equation, and any set of numbers, subject only to the above conditions, as the numbers belonging to that root. To subject the numbers belonging to any root of the characteristic equation of A to any condition other than those given above, is of course, equivalent to imposing certain conditions upon the coefficients of A.

The real linear homogeneous group G, for n variables, and the group $\mathfrak{G}$ of real projective transformations in $(n-1)$-fold space are connected as follows. If the variables x_1, x_2, etc., are regarded as the homogeneous coördinates of a point in $(n-1)$-fold space, the real linear transformation A homogeneous in the x's determines a corresponding real projective transformation $\mathfrak{A}$ in $(n-1)$-fold space. In the determination of this projective transformation, we are concerned only with the ratios of the coefficients of A; consequently, the transformations A and ρA of group G (where ρ is any real number) correspond to the same projective transformation $\mathfrak{A}$. The identical transformation I and the transformation ρI of group G correspond to the same projective transformation $\mathfrak{E}$, the identical transformation of group $\mathfrak{G}$. Let B be a transformation of group G corresponding to the real projective transformation $\mathfrak{B}$: if $A = B^m$, then $\mathfrak{A} = \mathfrak{B}^m$; and, if $\mathfrak{A} = \mathfrak{B}^m$, then $\rho A = B^m$ for some real quantity ρ. Consequently, if either A or ρA is the m^{th} power of a transformation of group G, the corresponding projective transformation $\mathfrak{A}$ of group $\mathfrak{G}$ is the m^{th} power of some transformation of this group, and not otherwise. Further, if B is infinitesimal, the corresponding projective transformation $\mathfrak{B}$ differs infinitely little from the identical transformation of group $\mathfrak{G}$. Therefore, if either A or ρA can be generated by the repetition of an infinitesimal transformation of group G, the corresponding projective transformation of group $\mathfrak{G}$ can be generated by the repetition of an infinitesimal transformation of this group and not otherwise.

If $\overline{G}$ denotes the group of real linear transformations of determinant $+1$ homogeneous in n variables (the real special linear homogeneous group), every transformation $\overline{A}$ of group $\overline{G}$ determines a (corresponding) transformation of group $\mathfrak{G}$. If n the number of variables is odd, there is a one to one correspondence between the transformations of group $\overline{G}$ and the transformations of the real projective group. For in this case (that is, if n is odd), if A is a real linear transformation homogeneous in the variables corresponding to the real projective transformation $\mathfrak{A}$, the transformation $\overline{A} = \frac{1}{a} A$, where a denotes the real n^{th} root of the determinant of A, is a transformation of group $\overline{G}$ and the only transformation of this group the ratios of whose coefficients are the same as the ratios of the coefficients of

A. Consequently, when n is odd, if $\overline{A}$ is the m^{th} power of a transformation of group G, the corresponding real projective transformation $\mathfrak{A}$ is the m^{th} power of a transformation of group $\mathfrak{G}$ and conversely; also if $\overline{A}$ can be generated by the repetition of an infinitesimal transformation of group G, $\mathfrak{A}$ can be generated by the repetition of an infinitesimal transformation of group $\mathfrak{G}$, and conversely. On the other hand, if n is even, and if the determinant of A (the real linear transformation homogeneous in the variables, determining the real projective transformation $\mathfrak{A}$) is positive, there are corresponding to $\mathfrak{A}$ two transformations of group $\overline{G}$ obtained by dividing each coefficient of A by either the positive or by the negative real n^{th} root of the determinant of A; but if the determinant of A is negative there is no transformation of group $\overline{G}$ corresponding to $\mathfrak{A}$.

§ 2.*

In the *Comptes Rendus*, volume 94, Sylvester showed that every transformation A of non-zero determinant is the m^{th} power for any positive integer m of some transformation B. That is, if A is any transformation of non-zero determinant, a transformation B can always be found, for any positive integer m, such that $A = B^m$. In his paper, Sylvester also gave a formula expressing the coefficients of B as algebraic functions of the coefficients of A. From a subsequent theorem of Sylvester's,† it follows that, if m is sufficiently great, we may take B to differ as little as we please from the identical transformation.

For real linear transformations homogeneous in n variables we have the following theorems.

Theorem I. *If the transformation A is real and of non-zero determinant (or of determinant $+1$), a real transformation B of non-zero determinant (or of determinant $+1$) can always be found of which A is the $(2m+1)^{th}$ power for any odd number $2m+1$. But in order that A may be any even power of a real transformation B of non-zero determinant (or of determinant $+1$), it is necessary and sufficient that all the numbers belonging to each negative root of the characteristic equation of A shall be even. Therefore, in order that the real transformation A of non-zero determinant (or of determinant $+1$) may be any even power of a real transformation B of non-zero determinant (or of determinant*

* Throughout this section, by transformation is meant a linear transformation homogeneous in n variables.

† *Johns Hopkins University Circulars.*

$+1$) *it is necessary and sufficient that* A *shall be the second power of a real transformation of non-zero determinant (or of determinant* $+1$).

Theorem II. *If* A *is the second power of a real transformation of non-zero determinant (or of determinant* $+1$), *a real transformation* B *of non-zero determinant (or of determinant* $+1$) *can always be found which shall be as nearly as we please equal to the identical transformation, and such that for some positive integer* m *sufficiently great* B^m *shall be equal to* A. *Consequently, any transformation that is the second power of a real transformation of non-zero determinant can be generated by the repetition of a real infinitesimal transformation; and, in particular, a transformation that is the second power of a real transformation of determinant* $+1$ *can be generated by the repetition of an infinitesimal transformation of determinant* $+1$.

Theorem III. *If the real transformation* A *of non-zero determinant (or of determinant* $+1$) *is not the second power of a real transformation of non-zero determinant (or of determinant* $+1$), *nevertheless, a real transformation* B *of non-zero determinant (or of determinant* $+1$) *can be found whose coefficients are algebraic functions of a parameter* t *such that* A *shall be the limit towards which the transformation* B^2 *approaches as* t *approaches zero, provided the multiplicity of each negative root of the characteristic equation of* A *is even.*

If λ is any root of the characteristic equation of the real transformation B, and if, for $r, s=1, 2, \cdots n$,

$$|1-b_{rr}|<\varepsilon, \quad |b_{rs}|<\varepsilon \ (r \neq s),$$

where ε is any positive quantity, then provided ε is sufciently small, the absolute value of $1-\lambda$ may be made as small as we please; and consequently no root of the characteristic equation of B will be negative or equal to zero. Therefore, by *Theorem* I, if ε is sufficiently small, B is the second power of a real transformation B_1 of non-zero determinant; and, in particular, if B is of determinant $+1$, B_1 may be so chosen that its determinant shall be equal to $+1$. For any positive integer m, B^m is equivalent to the second power of B_1^m; that is, $B^m=(B_1^2)^m=(B_1^m)^2$. Whence we have the following theorem.

Theorem IV. *The repetition of a real infinitesimal transformation results in a transformation which is the second power of a real transformation. In particular, the repetition of a real infinitesimal transformation of determinant* $+1$ *results in a transforma-*

tion which is the second power of a real transformation of determinant $+1$.

From *Theorem* III follows:

Theorem V. *By the repetition of a real infinitesimal transformation, we may approach as near as we please to any real transformation A of non-zero determinant, provided the multiplicity of each negative root of the characteristic equation of A is even. In particular if these conditions are satisfied, and if the determinant of A is $+1$, we may approach as near as we please to A by the repetition of a real infinitesimal transformation of determinant $+1$.*

If the transformation A is not the second power of a real transformation, it may be that $-A$ is the second power of a real transformation. The roots of the characteristic equation of $-A$ are the negatives of the roots of the characteristic equation of A. Whence follows from *Theorem* I:

Theorem VI. *In order that the real transformation $-A$ of non-zero determinant shall be the second power of a real transformation, it is necessary and sufficient that the numbers belonging to each positive root of the characteristic equation of A shall all be even.*

§ 3.

In the *Bulletin* for July, 1894, I pointed out that not every orthogonal substitution can be generated by the repetition of an infinitesimal orthogonal substitution, and if G is the group of proper orthogonal substitutions I showed that

Theorem VII. *If we designate a transformation of the group G as of the first or second kind according as it is or is not the second power of a transformation of the group, then every transformation of the first kind is the m^{th} power of a transformation of the group for any positive integer m, and can be generated by the repetition of an infinitesimal transformation of the group. By definition no transformation of the second kind is any even power of a transformation of the group. Nor can any transformation of the second kind be generated by the repetition of an infinitesimal transformation of the group. But every transformation of the second kind is the $(2m+1)^{th}$ power of a transformation of the group for any odd exponent $2m+1$.*

In a note at the end of this paper, I mentioned that *Theorem* VII was true of the group of linear transformations homogeneous in n variables that transform into itself a bilinear form (of non-zero determinant understood) with co-

grediant variables. This was afterwards demonstrated for an alternate bilinear form in a paper published in volume 46 of the *Mathematische Annalen*.

In a paper presented to the *American Academy of Arts and Sciences*, April, 1895, I have shown that *Theorem* VII holds for the *class* of linear transformations homogeneous in n variables that transform a bilinear form (of non-zero determinant) with contragrediant variables into itself. The transformations of this class that are commutative form a a group for which also *Theorem* VII holds.

My attention has recently been called to a note in the *Bulletin* for November, 1893,* stating that Professors Engel and Study have found that not every transformation of the special linear homogeneous group for two variables can be generated by the repetition of an infinitesimal transformation of that group. There is nothing in the note to show that the *real* special linear homogeneous group is referred to.†

I learn from Prof. H. B. Newson that he has found that not every transformation of the real projective group can be generated by the repetition of an infinitesimal transformation of that group. This discovery suggested the extension of *Theorem* VII to other sub-groups of the projective group. It follows at once from Newson's discovery that not every transformation of the real linear homogeneous group can be generated by the repetition of an infinitesimal transformation of this group; and further that not every transformation of the real special linear homogeneous group for an odd number of variables can be generated by the repetition of an infinitesimal transformation of this group. For could every transformation of either of these groups be generated by the repetition of an infinitesimal transformation of that group, then, as pointed out in § 1, every transformation of the real projective group could be generated by the repetition of an infinitesimal transformation of this group, which is not the case.

It follows from *Theorems* I, II and IV, that *Theorem* VII is true for the real linear homogeneous group for n variables,

* Page 66.

† *Theorem* VII holds for the special linear homogeneous group in two variables; and the transformation $x' = -x + y$, $y' = -y$ is not the second power of a transformation of this group, and therefore cannot be generated by the repetition of an infinitesimal transformation of this group. From the note it would appear that the identical transformation $x' = x$, $y' = y$, and the involutional transformation $x' = -x$, $y' = -y$ can not be generated by the repetition of an infinitesimal transformation of the group, which is erroneous.

and also for the group of real linear transformations of determinant $+1$ homogeneous in n variables (the real special linear homogeneous group); and, from what is stated in the latter part of § 1, that *Theorem* VII holds for the real projective group.

In volume 26, page 364 of the *Proceedings of the London Mathematical Society*, I have shown that in order that an orthogonal substitution may be of the first kind (that is, in order that a transformation of the orthogonal group may be generated by the repetition of an infinitesimal orthogonal transformation), it is necessary and sufficient that either -1 shall not be a root of the characteristic equation of the substitution or that the numbers belonging to the root -1 shall all be even. In a paper read at the Summer Meeting, 1895, of the *American Mathematical Society* (to appear in the *Quarterly Journal of Mathematics*) I showed that a transformation of the group of linear transformations homogeneous in the variables that transform an alternate bilinear form with cogrediant variables into itself will be of the first kind under the same conditions.*

By *Theorem* I, in order that a transformation of the real linear homogeneous group (or of the real special linear homogeneous group) shall be of the first kind it is necessary and sufficient that the numbers belonging to each negative root of the characteristic equation of the transformation shall all be even.

Therefore, by § 1, in order that a transformation of the real projective group shall be of the first kind, it is necessary and sufficient, either that the numbers belonging to each positive root of the characteristic equation of the transformation shall all be even, or else that the numbers belonging to each negative root of the characteristic equation shall all be even; provided there are both positive and negative real roots. Otherwise no condition is necessary.

In the article in the *Bulletin* on orthogonal substitution above mentioned I showed that by the repetition of an infinitesimal orthogonal substitution we can approximate as nearly as please to any proper orthogonal substitution of the second kind. In the above mentioned paper in the *Mathematische Annalen* I showed that by the repetition of an

* In the paper I also showed that every orthogonal transformation of this group is of the first kind. Also, if $\mathfrak{F}$ denotes a bilinear form of non-zero determinant with cogrediant variables, and $\mathfrak{F}'$ its conjugate; and if neither the determinant of $\mathfrak{F}+\mathfrak{F}'$ nor of $\mathfrak{F}-\mathfrak{F}'$ is zero, that then every linear transformation homogeneous in the variables that transforms $\mathfrak{F}$ into itself is the m^{th} power of such a transformation for any exponent m.

infinitesimal transformation of the group of linear transformations homogeneous in the variables that transform an alternate bilinear form into itself we can approximate as nearly as we please to any transformation of the second kind belonging to this group.

From *Theorem* V it follows that by the repetition of an infinitesimal transformation of the real linear homogeneous group (or of the real special linear homogeneous group) we may approximate as nearly as we please to any transformation of the second kind belonging to this group, provided the multiplicity of each negative root of the characteristic equation of this transformation is even.

Therefore by the repetition of an infinitesimal transformation of the real projective group we may approximate as nearly as we please to any transformation of the second kind belonging to this group, provided that either the multiplicity of each positive root of the characteristic equation of this transformation is even or else that the multiplicity of each negative root of the characteristic equation is even.

Worcester, Mass.

POSTSCRIPT.

The general real linear group and the special real linear group. The totality of linear transformations

$$y_r' = \mathbf{a}_{r1}\, y_1 + \mathbf{a}_{r2}\, y_2 + \cdots + \mathbf{a}_{r,\, n-1}\, y_{n-1} + \mathbf{a}_{r,\, n} \quad (r = 1, 2, \cdots n-1)$$

for which the determinant $\Sigma \pm \mathbf{a}_{11}\, \mathbf{a}_{22} \cdots \mathbf{a}_{n-1,\, n-1}$ is not zero form a group termed by Lie the *general linear group*. The sub-group of transformations for which the determinant $\Sigma \pm \mathbf{a}_{11}\, \mathbf{a}_{22} \cdots \mathbf{a}_{n-1,\, n-1}$ is $+1$, Lie terms the *special linear group*. These two groups are obviously identical with the two groups of linear transformations A that are respectively of non-zero determinant and of determinant $+1$, homogeneous in n variables and defined by the equations

$$x_r' = a_{r1}\, x_1 + a_{r2}\, x_2 + \cdots + a_{rn}\, x_n \quad (r = 1, 2, \cdots n-1),$$
$$x_n' = x_n,$$

For the general real linear group, and for the special real linear group, *Theorem* VII holds.* The conditions neces-

* Every transformation of the general linear group is the m^{th} power of a transformation of this group for any exponent m, and can be generated by the repetition of an infinitesimal transformation of this group, if we consider transformation of this group both imaginary and real. The same is true of the special linear group.

sary and sufficient that a transformation A of the general real linear group (or of the special real linear group) may be of the first kind are that the numbers belonging to each negative root of the characteristic equation of A shall all be even. By the repetition of an infinitesimal transformation of the real linear group we may approximate as nearly as we please to any transformation A of the second kind belonging to this group, provided the multiplicity of each negative root of the characteristic equation of is A even, but not otherwise. In particular, if these conditions are satisfied (but not otherwise), and if A is of determinant $+1$, we may approximate as nearly as we please to A by the repetition of an infinitesimal transformation of the special real linear group.

Special linear homogeneous group. Let A be any linear transformation (real or imaginary) of determinant $+1$ homogeneous in n variables, that is, let A be any transformation of the special linear homogeneous group. Let

$$\lambda'=r_1 e^{\theta_1\sqrt{-1}}, \qquad \lambda''=r_2 e^{\theta_2\sqrt{-1}}, \text{ etc.},$$

(where θ_1, θ_2, etc., are the smallest positive arguments of λ', λ'', etc.,) be the roots of the characteristic equation of A of respectively multiplicity m', m'', etc. Since the determinant of A is $+1$, we have

$$r_1^{m'} r_2^{m''} \cdots\cdots = 1,$$
$$m'\theta_1 + m''\theta_2 + \cdots\cdots = 2k\pi,$$

for some positive integer k.

If $k=0$, the transformation A can be generated by the repetition of an infinitesimal transformation of the special linear homogeneous group. The conditions in general necessary and sufficient in order that A may be generated by the repetition of an infinitesimal transformation of this group are somewhat complicated; they depend upon k, and upon the numbers belonging to the roots λ of the characteristic equation of A. The conditions may be exhibited as follows.

Let the numbers belonging to λ' be

$$m_1', m_2', \cdots\cdots m'_{\nu'-1}, m'_{\nu'} = m';$$

let the numbers belonging to λ'' be

$$m_1'', m_2'', \cdots\cdots m''_{\nu''-1}, m''_{\nu''} = m'';$$

etc., etc. Form a diagram corresponding to λ' by arranging m' dots in rows and columns so that there shall be ν' rows respectively of

$$m_1', m_2'-m_1', \cdots\cdots m'_{\nu'}-m'_{\nu'-1},$$

dots. The number of columns will then be m'_1. In one column there will be ν' dots. Let the number of dots in these m_1' columns be respectively

$$p_1', p_2', \cdots\cdots p'_{m'_1}.$$ *

* If the numbers belonging to λ' are 5, 9, 13, 16, the diagram corresponding to λ' is

* * * * *
* * * *
* * * *
* * *

and $$p_1'=p_2'=p_3'=4, \quad p_4'=3, \quad p_5'=1,$$

Next form a diagram corresponding to λ'' by arranging m'' dots in rows and columns so that there shall be ν'' rows respectively of

$$m_1'', m_2''-m_1'', \cdots\cdots m''_{\nu''}-m''_{\nu''-1},$$

dots; and let the number of dots in these m_1'' columns be respectively

$$p_1'', p_2'', \cdots\cdots p''_{m''_1}.$$

Proceed in the same way to form diagrams corresponding to the other roots of the characteristic equation of A.

Let now δ be the greatest common divisor of the p's. *Then if k contain δ, A can be generated by the repetition of an infinitesimal transformation of the special linear homogeneous group and not otherwise.* In particular, if m', m'', etc., have no common factor, A can be generated by the repetition of an infinitesimal transformation of the special linear homogeneous group.

If the transformation A can be generated by the repetition of an infinitesimal transformation of the special linear homogeneous group, A is the m^{th} power of a transformation of this group for any exponent m.

If δ_1 is the greatest common divisor of k and δ, then A is the m^{th} power of a transformation of the special linear homogeneous group for any exponent m that contains no factor of δ except a factor of δ_1; but for no other exponent is A

the m^{th} power of a transformation of the special linear homogeneous group. In particular if m is relatively prime to n, the number of variables, A is the m^{th} power of a transformation of the special linear homogeneous group.

If A cannot be generated by the repetition of an infinitesimal transformation of the special linear homogeneous group, the m^{th} power of A can be generated thus, provided m contains δ/s_1 (the quotient of δ by the greatest common divisor of δ and k), but not otherwise.

March 4, 1896.

NOTES.

A REGULAR meeting of the American Mathematical Society was held in New York on Saturday afternoon, February 29, at three o'clock, the President Dr. HILL, in the chair. There were eleven members present. On the recommendation of the Council, Mr. HARRY BROWN EVANS, University of Pennsylvania, Philadelphia, Pa., was elected to membership. The following papers were read:

(1) Professor M. I. PUPIN: "On the integral of the differential equation

$$a\frac{d^2y}{dt^2} + b\frac{dy}{dt} = c\frac{d^2y}{dx^2}$$

under certain boundary conditions occurring in the theory of long electrical waves."

(2) Professor E. H. MOORE: "A two-fold generalization of Fermat's theorem."

In the absence of Professor Moore his paper was read by the Secretary.

AMONG the courses for the summer semester at Berlin are the following—Professor Fuchs: Introduction to the theory of differential equations; Introduction to the theory of functions;—Professor Frobenius: Theory of numbers (second course); Theory of determinants;—Professor Schwarz: Analytical geometry; Applications of the theory of the elliptic functions; Hyper-geometric series; Mathematical colloquium;—Professor Knoblauch, Theory of the elliptic functions; Theory of curved surfaces; Theory of space curves; —Professor Hettner: Introduction to the theory of infinite series, products, and continued fractions;—Professor Hensel: Concerning the transcendentalism of e and π; Higher alge-

bra (group and substitution theories);—Dr. Schlesinger: Geometry of three dimensions (synthetic and analytic); Differential calculus and introduction to analysis; Exercises in the differential calculus;—Dr. Kötter: Integral calculus; Focal properties of surfaces of the second order; Exercises in the integral calculus;—Dr. Hoppe: Integral calculus; Analytical mechanics;—Dr. Arons: Application of the differential and integral calculus to physical and chemical problems;—Dr. Glan: Quaternions.

AMONG the courses for the summer semester at Göttingen are the following:—Professor Schering: Mechanics;—Professor Klein: Special topics in the theory of numbers; Concerning problems in applied mechanics;—Professor Schur: Numerical calculation and applications to the method of least squares;—Professor Burkhardt; Elliptic functions;—Professor Hilbert; Theory of ordinary differential equations; Concerning the squaring of the circle;—Professor Schönflies: Analytical geometry; Special topics in the theory of functions;—Dr. Sommerfeld: Theory of surfaces, Exercises in the theory of surfaces;—Dr. Bohlmann: Differential calculus.

THE French Association for the Advancement of Science holds its annual meeting this year at Tunis, April 1–4; E. Collignon is Chairman of Sections I and II (mathematics, mechanics, and astronomy).

A WORK of more than ordinary interest and originality has just been issued from the press of B. G. Teubner. It is the first volume of the *Geometrie der Berührungstransformationen, dargestellt von* SOPHUS LIE *und* G. SCHEFFERS. The authors give the following synopsis of the subjects treated in this volume:

"During the years 1869–71, Lie developed a geometrical theory of contact transformations and explained by means of it the mutual connection and interrelation between projective and metrical geometry. At the same time he showed the fertility of this theory by numerous applications to partial differential equations of the first and second orders. The present work is intended to give a full presentation of these theories.

It has been attempted to present the subject in such a form as to make it intelligible not only to the professional mathematician but even to students who are acquainted merely with the more elementary branches of higher mathematics.

The first volume is divided into three parts. In the *first part* it is shown how, in the course of time, the idea of

point transformations was introduced and applied in geometry. Particular attention is here given to the first contact transformation ever introduced into mathematics, viz., dilatation, which really lies at the basis of Huygens's theory of waves. Next the transformations by means of pedals and reciprocal polars are treated. After these and other examples, the general idea of the *contact transformation in the plane* is defined both analytically and geometrically and its theory is fully developed.

The importance of the theory of *infinitesimal* contact transformations is finally illustrated by an elegant and difficult problem: to determine the form of the element of arc for all those surfaces on which the system (Schaar) of geodesic circles admits a continuous system of contact transformations or a discrete number of point transformations.

While the first part contains a theory of the transformations of line elements in the plane, the *second part* is intended to give a *geometry of line elements in space*. This geometry comprises the *Pfaffian equations* and expressions closely connected with the *null-systems*, and the *Mongian equations* $\Omega(x, y, z; dx, dy, dz) = 0$ to which Plücker's *line complexes* are intimately related. All these theories appear here from a new point of view, as parts of the same whole. To illustrate the wide applicability of these views a theory of the *tetrahedral complexes* is given and a number of important categories of *partial differential equations* of the second order are integrated.

The central point of the discussions of the second part will again be found in its last chapter where an important polar relation between two spaces is investigated, each space containing a certain line complex whose lines correspond to the points of the other space. This establishes a correspondence between the surface elements of the two spaces which is really a *contact transformation in space transforming straight lines into spheres and asymptotic curves into lines of curvature*. This at once transforms Plücker's line geometry into a sphere geometry.

The *third part* introduces the *geometry of surface elements*. First, Lagrange's theory of *partial differential equations of the first order* is developed geometrically, according to Monge. It is then shown how much this theory gains in simplicity through the introduction of the surface element as a fundamental idea. Then follows the consideration of partial differential equations of the first order admitting infinitesimal point transformations; finally, a series of categories of such equations, of special interest in geometry, is investigated."

NEW PUBLICATIONS.

HIGHER MATHEMATICS.

BOLYAI (J.). The science absolute of space, independent of the truth or falsity of Euclid's axiom XI (which can never be decided *a priori*). Translated from the Latin by G. B. Halsted. 4th edition. Austin, Halsted, 1896. 12mo. 30 and 72 pp. Cloth. $1.00

BONETTI (E.). Alcune questioni sui contatti sferici, precedute da una esposizione sui centri, assi e piani di similitudine. Messina, 1895. 8vo. 12 pp.

CAYLEY (A.). Collected mathematical papers. (In 13 volumes.) Vol. 9. Cambridge University Press (Macmillan). 4to. 16 and 621 pp. $6.50.

DAUGE (F.). Cours de méthodologie mathématique. 2e édition, revue et augmentée. Gand, 1896. 8vo. 10 and 525 pp., 12 plates. Fr. 13.00

DURÈGE (H.). Elements of the theory of functions of a complex variable with especial reference to the methods of Riemann. Authorized translation from the fourth German edition by G. E. Fisher and I. J. Schwatt. Philadelphia, Fisher & Schwatt, 1896. 8vo. $2.50.

GAMBARDELLA (F.). Elementi di calcolo infinitesimale. 2a edizione. Livorno, Giusti, 1895. 8vo. 8 and 517 pp. Fr. 9.00

GERNET (M.). Ueber Reduktion hyperelliptischer Integrale. [Diss.] Heidelberg, 1895. 8vo. 40 pp.

GRANE (N.). Ueber Kurven mit gleichartigen successiven Developpoiden. Lund, 1894. 8vo. 71 pp. Mk. 2.50

GRIESS (J.). See KLEIN (F.).

HACK (F.). Beiträge zur Anwendung der Gruppentheorie auf kubische und biquadratische Gleichungen. [Diss.] Tübingen, 1895. 8vo. 36 pp.

HALLGREN (E.). Om Beräkningen af Abelska Integralers Omvändning. Göteborg, 1894. 8vo. 78 pp., 7 plates. Mk. 3.00

HALSTED (G. B.). See BOLYAI (J.).

HANSEN (P.C.V.). Et Brudstykke af den analytiske Plangeometri. Kjöbenhavn, 1895. 4to. 48 pp. (Lithographed.) Mk. 1.80

KLEIN (F.). Leçons sur certaines questions de géométrie élémentaire. (Possibilité des constructions géométriques; les polygones réguliers; transcendance des nombres e et π). Rédaction française par J. Griess. Paris, Nony, 1895. 8vo.

KÖNIGSBERGER (L.). Hermann von Helmholtz's Untersuchungen über die Grundlagen der Mathematik und Mechanik. Heidelberg, 1895. 4to. 70 pp.

KUMMELL (C. H.). To express the roots of the solvable quantics as symmetrical functions of homologues. (*American Journal of Mathematics*, Vol. 18, pp. 74–94.) 4to.

LIEBMANN (H.). Die einzweideutigen Punktverwandtschaften der Ebene. [Diss.] Jena, 1895. 8vo. 52 pp.

MILDNER (R.). Ueber einige allgemeinere, durch einfache und Doppelintegrale ausdrückbare unendliche Reihen und Produkte. [Progr.] Znaim, 1895. 8vo. 18 pp.

MORAWETZ (J.). Zur analytischen Geometrie des Punktes und der Geraden. [Progr.] Salzburg, 1895. 8vo. 24pp.

NÜSSLEIN (T.). Ueber die ebenen Configurationen C_3. Leipzig, 1895. 8vo. 36 pp., 2 plates. Mk. 1.80

RATH (E.). Die Grundformeln der allgemeinen Kurven- und Flächentheorie im nichteuklidischen Raum. [Diss.] Tübingen, 1894. 8vo. 42 pp.

SCHLEGEL (V.). Die Grassmann'sche Ausdehnungslehre. Ein Beitrag zur Geschichte der Mathematik in den letzten fünfzig Jahren. (*Zeitschrift für Mathematik und Physik*, Vol. 41 (1896), historisch-literarische Abteilung, pp. 1-21.) 8vo.

————. Sur un systéme de coordonnées tétraédriques. (*Nouvelles annales de mathématiques*, série 2, Vol. 11., pp. 70-74.) 8vo.

SCHOTTEN (H.). Der Koördinatenbegriff und die analytische Geometrie der Kegelschnitte. Berlin, Grote, 1895.

II. ELEMENTARY MATHEMATICS.

ADLER (A.). Zur Theorie der geometrischen Konstruktionen. [Progr.] Pilsen, 1895. 8vo. 11 pp.

ALBRECHT (T.). See BREMIKER (C.).

ANDEREGG (F.) and ROE (E. D.). Trigonometry for schools and colleges. Boston, Ginn, 1896. 16mo. 8 and 188 pp. $0.80

BARBERIS ed OTTINI. Sviluppo, costruzione e misurazione dei solidi geometrici. Torino, 1896. 8vo. 14 plates. Fr. 1.00

BREMIKER (C.). Logarithmisch-trigonometrische Tafeln. Neu bearbeitet von T. Albrecht. 12te Ausgabe. Berlin, 1895. 8vo. 18 and 598 pp. Mk. 4.20

BÜTTNER (A.). Elemente der Buchstabenrechnung und Algebra; nebst Anhang: Logarithmentafeln für die Zahlen von 1 bis 10,000. 12te Auflage. Bielefeld, 1896. 8vo. 4 and 192 pp. Cloth. Mk. 3.20

CAPEL (A. D.). Common sense Euclid. Part I: Books 1 and 2, with 300 problems. 4th edition, revised and enlarged. Part II: Books 3 and 4, with 300 problems. London, Abbott, 1896. 12mo. 156 and 140 pp. 1s. 6d. and 2s.

CLARKE (A. D.). Mensuration for the use of schools and Woolwich, Sandhurst, and Home Civil Service candidates. With numerous examples, solutions, and answers. London, 1895. 8vo. 96 pp. Cloth. 3s.

CUSACK. See SMITH (H. J.).

DUFAILLY (J.). Géométrie. 9e édition. Paris, 1895. 8vo. 432 pp. Fr. 4.00

FREELAND (W.). Algebra for schools and colleges. New York, Longmans, 1896. 8vo. 320 pp. $1.40

GREMEGNI (M.). Sull' equivalenza dei poligoni piani e sferici; dimostrazione di un assioma d'Euclide. Firenze, Bemforad, 1895. 8vo. 20 pp.

———. Aggiunte e note alla teoria dei poligoni equivalenti. Firenze, Bemforad, 1895. 8vo. 8 pp.

GREVE (A.). Fünfstellige logarithmische und trigonometrische Tafeln, nebst einer grösseren Anzahl von Hilfstafeln. 6te Auflage. Bielefeld, 1896. 8vo. 4 and 174 pp., 1 plate. Cloth. Mk. 2.00

HALL (L.). The elements of algebra. New York, American Book Co., 1895. 12mo. 368 pp. Half leather. $1.00

HANSON (C.). Elementaer Plangeometri. 2te udgave. Hjörring, 1895. 8vo. 112 pp. Cloth. Mk. 2.20

HORNBROOK (A. R.). Concrete geometry for beginners. New York, American Book Co., 1896. 12mo. 201 pp. $0.75

JONES (G. W.). A drill-book in trigonometry. 6th edition. Ithaca, N. Y., Jones, 1896. 12mo. 16 and 192 pp. Cloth. $1.00

KÖSTER (T. E.). Aufgaben aus dem Gebiete der Arithmetik und Algebra für Mittelschulen. Teil 1. 2te Auflage. Oldenburg, Schulze, 1896. 8vo. 4 and 96 pp. Mk. 0.80

KUSCHNIRIUK (M.). Ueber Kombinationen zu bestimmten Summen. [Progr.] Mährisch-Trübau, 1895. 8vo. 20pp.

MACNAB (S.). Trigonometry simplified: Solution of all plane and spherical triangles and application of the same to the various problems in navigation and nautical astronomy. London, Philip, 1896. 8vo. 24 pp. 1s.

MACNIE (J.). Elements of plane geometry. Edited by White. New York, American Book Co., 1896. 12mo. 240 pp. Half leather. $0.75

MEIGEN (F.). Lehrbuch der Trigonometrie. (Technische Lehrhefte, Mathematik, Heft 5.) Hildburghausen, Pezoldt, 1896. 8vo. 4 and 60 pp. Mk. 1.30

MITCHESON (T.). Examples in algebra. London, Hodgson, 1896. 8vo. 80 pp. 1s.

———. Answers to the Examples in algebra. London, Hodgson, 1896. 8vo. 42 pp. 1s.

OTTINI. See BARBERIS ed OTTINI.

ROE (E. D.). See ANDEREGG (F.) and ROE (E. D.).

SCHURIG (R.). Katechismus der Algebra. 4te, vollständig neu bearbeitete Auflage. Leipzig, Weber, 1896. 8vo. Cloth. Mk. 3.00

SMITH (H. J.). Cusack's mensuration. London, London Book Depot, 1896. 8vo. 256 pp. 2s. 6d.

STERZA (A.). La matematica per il terzo anno delle scuole tecniche: aritmetica razionale, calcolo letterale e geometria. Mantova, Mondovi, 1895. 8vo. 214 pp. Fr. 2.50

TESTI (G. N.). Elementi di geometria, con una raccolta di 510 esercizi e problemi. 3a edizione, riveduta. Livorno, Giusti, 1895. 16mo. 16 and 240 pp. Fr. 1.75

WHITE. See MACNIE (J.).

III. APPLIED MATHEMATICS.

ARNDT (L.). Beitrag zur Berechnung der störenden Kräfte in der Theorie der säcularen Störungen. [Diss.] Berlin, 1895. 8vo. 44 pp.

ASCHIERI (F.). Lezioni di geometria descrittiva. 2a edizione. Milano, Hoepli, 1895. 8vo. 456 pp. Fr. 8.50

BRENT (C.), WALTER (A. F.), and WILLIAMS (G.). Ex-meridian altitude tables (declination 0° to 70°), to which is added an explanation of maximum altitudes, etc. London, Philip, 1896. 8vo. 92 pp. 5s.

ELLINGER (H. O. G.). Laerebog om Lyset. Geometrisk Optik. Kjöbenhavn, 1895. 8vo. 118 pp. Mk. 2.80

GLAZEBROOK (R. T.). James Clerk Maxwell and modern physics. London, Cassell, 1896. 8vo. 6 and 224 pp. Cloth. 3s. 6d.

GOUILLY (A.). Géométrie descriptive. (En 3 parties.) Partie I: Point, ligne droite, plan. Paris, 1896. 8vo. 164 pp. Fr. 2.00

GUYON (E.). Les problèmes de navigation et la carte marine. Types de calculs et tables complètes. Paris, Imprimerie nationale, 1895. 8vo. 106 pp. 2 plates.

HAMON (G.) Histoire générale de l' assurance en France et á l' Etranger. Fascicules 1—4. Paris, 1895. 8vo. Pp. 1—160. Fr. 8.00

HANCOCK (H.). Text-book of mechanics and hydrostatics. New York, Van Nostrand, 1895. 12mo. 408 pp. Cloth. $1.75

HARZER (P). Die säkularen Veränderungen der Bahnen der grossen Planeten. (Preisschrift der Jablonowskischen Gesellschaft.) Leipzig, Weidmann, 1895. 8vo. 26 and 280 pp. Mk. 12.00

JAHRBUCH für das deutsche Versicherungswesen 1896. Lebens-, Renten- und Unfallversicherung nebst vergleichenden Tabellen der Prämien deutscher Lebensversicherungs-Gesellschaften. Herausgegeben von J. Neumann. Berlin, 1896. 12mo. 8 and 536 and 48 pp. Cloth. Mk. 10.00

LOUDON (W. J.). An elementary treatise on rigid dynamics. New York, Macmillan, 1896. 8vo. 10 and 236 pp. Cloth. Mk. 2.25

LUEGER (O.). Lexikon der gesammten Technik und ihrer Hilfswissenschaften. Im Verein mit Fachgenossen herausgegeben. (In ca. 5 Bänden.) Vol. II. Stuttgart, Deutsche Verlags-Anstalt, 1895. Mk. 30.00

MANEUVRIER (G.). Traité élémentaire de mécanique rationnelle et appliquée. Paris, Hachette, 1896. 16mo. 320 pp. Fr. 4.00

NEUMANN (J.). See JAHRBUCH.

SEE (T. J. J.). Researches on the orbit of F. 70 *Ophiuchi*, and on a periodic perturbation in the motion of the system arising from the

action of an unseen body. (*The Astronomical Journal*, Vol. 16, pp. 17–28). 4to.

TABLES de mortalité du comité des compagnies d'assurances à primes fixes sur la vie (Compagnie d'assurances générales, Union nationale et Phénix). Paris, 1895. 4to. 56 and 416 pp., 3 plates. Cloth. Fr. 50.00

TOMBECK (H. E.). Éléments de géométrie descriptive. 7e édition. Paris, Hachette, 1896. 8vo. 130 pp. Fr. 2.50

WALTER (A. F.). See BRENT (C.).

WEBB (W. L.). Problems in the use and adjustment of engineering instruments. New York, Wiley, 1896. 16mo. $1.00

WILLIAMS (G.). See BRENT (C.).

ZEUTHEN (H. C.). Forelæsninger over Bevægelseslære ved Polyteknisk Læreanstalt. Kjöbenhavn, 1895. 8vo. 116 pp. Mk. 2.50